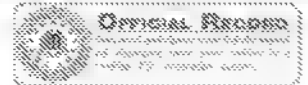


~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Electronic Communication

**Title:** (U//~~FOUO~~) Missing Item - [REDACTED]  
302-1A20

**Date:** 05/06/2019

b3  
b7E

**From:** WASHINGTON FIELD  
WF-CI13

**Contact:** [REDACTED]

b6  
b7C

**Approved By:** SSA [REDACTED]

**Drafted By:** [REDACTED]

**Case ID #:** [REDACTED] (U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3  
b7E

**Synopsis:** (U//~~FOUO~~) To document missing item [REDACTED]-302-1A20, which is described as "FD-597 Receipt for Property" acquired from Williams & Connolly LLP

~~Reason: 1.4(c)  
Derived From: Multiple  
Sources  
Declassify On: 20441231~~

**Reference:** [REDACTED]-302 Serial 23

b3  
b7E

### Details:

(U//~~FOUO~~) For reference, Washington Field Office (WFO) CI-13 has been gathering and copying materials from captioned case in response to a Freedom of Information Act (FOIA) tasking from Information Management Division (IMD; formerly Records Management Division).

(U//~~FOUO~~) On or about February 4, 2019, Special Agents (SAs) [REDACTED] [REDACTED] attempted to locate [REDACTED]-302-1A20, described as described as "FD-597 Receipt for Property" acquired from Williams & Connolly LLP (see referenced serial). The SA's looked

b3  
b6  
b7C  
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U//~~FOUO~~) Missing Item - [REDACTED]-302-1A20  
Re: [REDACTED]/06/2019

b3  
b7E

through all case materials in the CI-13 file and workbox area, however, they were not able to locate this item.

(U//~~FOUO~~) SA [REDACTED] inquired with Supervisory Intelligence Analyst (SIA) [REDACTED] regarding the item, as he was previously the IA assigned to the case. He was also not able to locate this item.

b6  
b7C

(U//~~FOUO~~) As such, WFO CI-13 considers the item missing and will enclose this document into 1A20 as a placeholder until the missing item is located.

◆◆

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1353814-0

Total Deleted Page(s) = 6

Page 92 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;  
Page 93 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;  
Page 94 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;  
Page 95 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;  
Page 96 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;  
Page 97 ~ b1 - Per CIA; b3 - Per CIA; b6 - Per CIA;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1/12/86  
Serial 130

b6 per  
b7C FBI

HRC-852



-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/7/2016

(U//~~FOUO~~) On January 7, 2016, writer received a 15 page fax from [redacted] Special Agent in Charge at the U.S. Department of State, Office of Inspector General. The faxed documents consisted of time and attendance records for Bryan Pagliano.

b6 per  
b7C DOS

(U//~~FOUO~~) The faxed documents are enclosed in an attached 1A.

Investigation on 1/7/2016 at Washington, DC

b3 per  
b7E FBI

File # [redacted] -130 Date dictated N/A

By FoA [redacted]

b6 per  
b7C FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-853

~~SECRET~~

HRC-858

~~SECRET~~

~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) ~~(S)~~ DOS

Date: 02/01/2016

Approved By: [REDACTED]

b6 per FBI  
b7C per FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED] (U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per FBI  
b7E per FBI

~~Reason: 1.4(b)  
Derived From: FBI  
NSISC-20090615  
Declassify On: 20261231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: Department of State

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type	Description
1B Digital	(U) 1 CD Marked [REDACTED] PST"
	Collected On: 01/28/2016
	Seizing Individual: [REDACTED]
	Located By: [REDACTED]
	Location Area: NA
	Specific Location: NA
	Device Type: Compact Disc/Digital Video Disc(CDs/DVDs)
	Number of Devices Collected: 1

b6 per DOS, FBI  
b7C per DOS, FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U)  
Title: ~~(S)~~ DOS

Re: [REDACTED] 02/01/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

~~SECRET~~

b3 per  
b7E FBI

HRC-861

~~SECRET~~

~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) EMAILS

Date: 02/03/2016

Approved By: [REDACTED]

b6 per FBI  
b7C per FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED] (U)

~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per FBI  
b7E per FBI

~~Reason: 1.4(c)~~

~~Derived From: Multiple  
Sources~~

~~Declassify On: 20411231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: [REDACTED] SPECIAL ASST, DEPT OF STATE

b6 per DOS  
b7C per DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type  
1B Digital

### Description

(U) 2 DVDS: OPENNER [REDACTED]-EMAIL - 2011.PST  
OPENNER [REDACTED]-EMAIL - 2012.PST  
Collected On: 02/03/2016  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: DEPT. OF STATE  
Specific Location: DEPT. OF STATE  
Device Type: Compact Disc/Digital Video  
Disc(CDs/DVDs)  
Number of Devices Collected: 2

b6 per DOS, FBI  
b7C per DOS, FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U) EMAILS

Re:  02/03/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

~~SECRET~~

HRC-864

~~SECRET~~



~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) ~~(S)~~ DVD provided by DoS

Date: 02/08/2016

Approved By: [Redacted]

b6 per  
b7C FBI

Drafted By: [Redacted]

Case ID #: [Redacted] (U) ~~(S)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per  
b7E FBI

~~Reason: 1.4(b)  
Derived From: FBI  
NSISC-20090615  
Declassify On: 20261231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: [Redacted]  
Department of State

b6 per  
b7C DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type	Description
1B Digital	(U) <del>(S)</del> DVD provided by Dos containing emails flagged during the FOIA process. Collected On: 02/05/2016 Seizing Individual: [Redacted] Collected By: [Redacted] Location Area: NA Specific Location: NA Device Type: Compact Disc/Digital Video Disc(CDs/DVDs) Number of Devices Collected: 1

b6 per  
b7C FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U) (S) DVD provided by DoS  
Re: [REDACTED] 02/08/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

~~SECRET~~

b3 per  
b7E FBI

HRC-867

~~SECRET~~

~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) DEPARTMENT OF STATE HQ

Date: 02/10/2016

Approved By: [REDACTED]

b6 per  
b7C FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per  
b7E FBI

~~Reason: 1.4(c)  
Derived From: Multiple  
Sources  
Declassify On: 20411231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: [REDACTED] DEPARTMENT OF STATE

b6 Per  
b7C DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type	Description
1B Digital	(U) ONE (1) DVD LABELED FIELD BM FILES AND MARKED SECRET. Collected On: 02/10/2016 Seizing Individual: [REDACTED] Collected By: [REDACTED] Location Area: DEPARTMENT OF STATE HQ Specific Location: ROOM 6316 Device Type: Compact Disc/Digital Video Disc(CDs/DVDs) Number of Devices Collected: 1

b6 per  
b7C FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U) DEPARTMENT OF STATE HQ

Re:  02/10/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

~~SECRET~~

HRC-870

~~SECRET~~



~~SECRET//NOFORN~~

# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) DEPARTMENT OF STATE

Date: 02/10/2016

Approved By: [REDACTED]

b6 per FBI  
b7C per FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED] (U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per FBI  
b7E per FBI

Reason: 1.4(c)  
Derived From: Multiple  
Sources  
Declassify On: 20411231

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: (U) [REDACTED]

b6 per DOS  
b7C per DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type  
1B Digital

### Description

(U) ONE (1) DVD LABELED [REDACTED] E-MAIL 2012  
Collected On: 02/10/2016  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: DEPARTMENT OF STATE HQ  
Specific Location: ROOM 6316  
Device Type: Compact Disc/Digital Video  
Disc(CDs/DVDs)  
Number of Devices Collected: 1

b6 per DOS, FBI  
b7C per DOS, FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U) DEPARTMENT OF STATE

Re:  02/10/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~



~~SECRET~~

HRC-873

~~SECRET~~

~~SECRET//NOFORN~~



# FEDERAL BUREAU OF INVESTIGATION

## Evidence Entry

Event Title: (U) DEPARTMENT OF STATE

Date: 02/10/2016

Approved By: [REDACTED]

b6 per FBI  
b7C per FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per FBI  
b7E per FBI

~~Reason: 1.4(c)  
Derived From: Multiple  
Sources  
Declassify On: 20411231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: [REDACTED]

b6 per DOS  
b7C per DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type  
1B Digital

### Description

(U) ONE (1) DVD LABELED [REDACTED] E-MAIL 2012  
Collected On: 02/10/2016  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: DEPARTMENT OF STATE  
Specific Location: ROOM 6316  
Device Type: Compact Disc/Digital Video  
Disc(CDs/DVDs)  
Number of Devices Collected: 1

b6 per DOS, FBI  
b7C per DOS, FBI

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Title: (U) DEPARTMENT OF STATE

Re:  02/10/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

2/12/16  
Serial 130

~~SECRET~~

b6  
b7C

HRC-876

~~SECRET~~

~~SECRET~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-02-2008 BY C66W46B11 NSICG

UNCLASSIFIED//~~FOUO~~

21 January 2016

b6  
b7C

MEMORANDUM FOR: [REDACTED]

Acting Section Chief  
Counterespionage Section  
Federal Bureau of Investigation

FROM: [REDACTED]

Associate Deputy Director of Operations  
Central Intelligence Agency,  
Foreign Intelligence and Covert Action

b3 Per CIA  
b6 Per CIA  
b7C Per CIA

SUBJECT: (U//~~FOUO~~) MIDYEAR EXAM:  
Use Request - 5 January 2016

(U//~~FOUO~~) By Letterhead Memorandum dated 5 January 2016  
you requested CIA approval to use emails surfaced in the  
referenced case with potential witnesses and their counsel. [REDACTED]

b1 Per CIA  
b3 Per CIA

[REDACTED] (S)  
(U//~~FOUO~~) I am the Associate Deputy Director of Operations  
for CIA, Foreign Intelligence and Covert Action. The content of  
the emails, which was described to me, involve operational  
matters within my jurisdiction. As such, I have the authority  
to grant approval to use these emails as outlined in the  
referenced use request and release of this memorandum provides  
that approval with the following caveats:

- FBI must verify that the witness/counsel:
  - o **had** the appropriate clearance contemporaneously with the sending/receipt of the email at issue;
  - o currently **has** the appropriate clearance when interviewed by the FBI; or
  - o signs a Non-disclosure Agreement at the time of the interview prior to being shown properly labeled CIA classified information.

[REDACTED]  
b3 Per CIA  
b6 Per CIA  
b7C Per CIA

Attachment: Requested emails

UNCLASSIFIED//~~FOUO~~

HRC-877

[REDACTED] 138

~~SECRET~~

b3  
b7E

~~SECRET~~

UNCLASSIFIED//~~FOUO~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-10-2016 BY J76J18T80 NSICG



**U.S. Department of Justice**  
**Federal Bureau of Investigation**  
Washington, D.C. 20535-0001

Date: 5 January 2016

To:

[Redacted]

Counterespionage Group  
Counterintelligence Center CIA

b3 Per CIA  
b6 Per CIA  
b7C Per CIA

From:

[Redacted]

Acting Section Chief  
Counterespionage Section

b6  
b7C

Subject: Requests authority use classified CIA documents during interviews

(U//~~FOUO~~) In July 2015, the FBI received a Section 811 referral from the Inspector General for the Intelligence Community (ICIG) regarding the possible compromise of classified national security information. The potential compromise was identified when, as part of a Freedom of Information Act (FOIA) request, the U.S. Department of State (DoS) and the [Redacted] reviewed electronic mail (email) communications from private email accounts previously used by a former Secretary of State during their tenure at DoS.

(U//~~FOUO~~) At the request of the FBI, as well DoS and the ICIG, the CIA has since conducted classification reviews of emails and documents related to this matter that were deemed to contain CIA equities.

(U//~~FOUO~~) Currently, the FBI plans to interview several individuals who originated, transmitted or received classified documents via an unclassified email system. During these interviews the FBI would like to show the interviewee, and if necessary their legal counsel, the relevant documents that they were a party to. Doing so will allow the FBI to pursue a logical line of questions regarding the circumstances in which the classified information was sent.

UNCLASSIFIED//~~FOUO~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~SECRET~~

HRC-878

~~SECRET~~

UNCLASSIFIED//~~FOUO~~

b1 Per CIA  
b3 Per CIA

×

(S)

(U//~~FOUO~~) As such, the FBI respectfully requests Central Intelligence Agency (CIA) authority to show the above referenced emails to those individuals that were originally involved in each respective email chain. Given the amount of time that has elapsed

UNCLASSIFIED//~~FOUO~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~SECRET~~

HRC-879

~~SECRET~~

UNCLASSIFIED//~~FOUO~~

Since the emails were first sent, the FBI believes that it is necessary to show the actual emails to the interviewees in order to have a meaningful discussion regarding the context in which the email was sent. For each listed email, the FBI will only show the email to individuals, and their attorneys, necessary to further the investigation. Additionally, standard safeguarding procedures will be used to ensure the protection of the content and to prevent any unnecessary disclosures.

(U//~~FOUO~~) Please direct all inquiries regarding this request to Special Agent [REDACTED]

b6  
b7C

Sincerely,

b6  
b7C

[REDACTED]  
Acting Section Chief  
Counterespionage Section

~~SECRET~~

UNCLASSIFIED//~~FOUO~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-880



2/12/16  
serial 139

~~SECRET~~

b6  
b7C

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100

HRC-881

~~SECRET~~

UNCLASSIFIED//~~FOUO~~

MEMORANDUM FOR:

[Redacted]

FEB 10 2016

b6  
b7C

Acting Section Chief  
Counterespionage Section  
Federal Bureau of Investigation

FROM:

[Redacted]

Information Review Officer for the Director's Area

b3 Per CIA  
b6 Per CIA  
b7C Per CIA

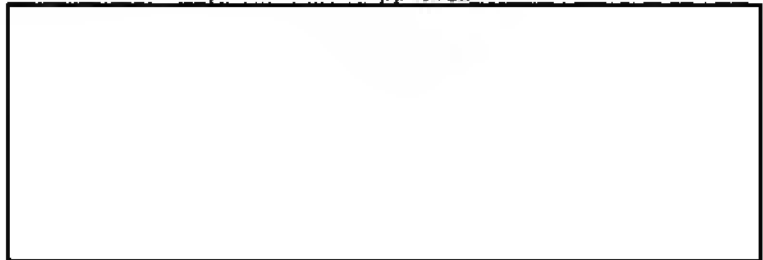
SUBJECT:

MIDYEAR EXAM: Use Request – 4 January 2016

(U//~~FOUO~~) By Letterhead Memorandum dated 4 January 2016 you requested CIA approval to use an email surfaced in the referenced case with two potential witnesses and their counsel. The email is unclassified, but for CIA Internal Use Only.

(U//~~FOUO~~) I am the Information Review Officer for the Director's Area and have Original Classification Authority. As such, I have the authority to grant approval to use this email as outlined in the referenced use request and release of this memorandum provides that approval.

b3 Per CIA  
b6 Per CIA  
b7C Per CIA



Attachment: Requested email

UNCLASSIFIED//~~FOUO~~

HRC-882

b3  
b7E

2/14/16  
Serial 140

b6 per  
b7C FBI

HRC-883

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/12/2016

b6 per DOS, FBI  
b7C per DOS, FBI

On February 12, 2016, SA [redacted] electronically sent the Department of State (Dos) an LHM requesting authority to use DoS emails and documents in future interviews regarding the captioned matter. The request was electronically sent to [redacted] Executive Assistant, Bureau of Diplomatic Security, [redacted]

Copies of the requests are maintained in a 1A.

Investigation on 2/12/2016 at Washington, DC

b3 per FBI  
b7E per FBI

File # [redacted] - 140 Date dictated N/A

By SA [redacted]

b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-884

2/26/16  
Serial 144

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

-----  
-----  
-----  
-----  
-----

LAW OFFICES  
**WILLIAMS & CONNOLLY LLP**

725 TWELFTH STREET, N.W.

WASHINGTON, D. C. 20005-5901

(202) 434-5000

FAX (202) 434-5029

DAVID E. KENDALL  
(202) 434-5145  
dkendall@wc.com

EDWARD BENNETT WILLIAMS (1920-1988)  
PAUL R. CONNOLLY (1922-1978)

February 22, 2016

BY E-MAIL

[REDACTED]  
U.S. Department of Justice  
National Security Division  
950 Pennsylvania Avenue NW  
Washington, DC 20530

b6 per  
b7C FBI

Dear [REDACTED]

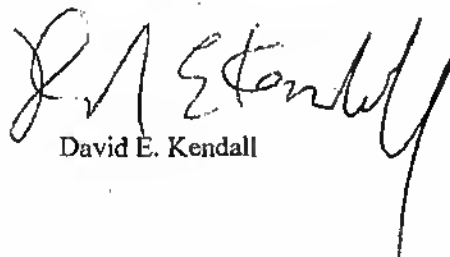
b6 per  
b7C FBI

I write to memorialize our responses to two inquiries concerning the Department of Justice's security inquiry.

You asked that we identify the serial numbers for the Williams & Connolly LLP ("W&C") laptops provided to the Federal Bureau of Investigation on August 6, 2015 and August 25, 2015, and to confirm the positions and number of W&C personnel who had access to those laptops during the time period that the laptops contained the .pst file of the e-mails that Secretary Clinton produced to the State Department. As listed on the property receipts for those laptops, the model and serial numbers are: (1) Lenovo Thinkpad T420, S/N PB-YC912 12/03; (2) Lenovo 4236-VQ5 S/N PB-YC910 12/03; and (3) Lenovo 4236-VQ5 S/N R8-NV8XB 11/11. Five W&C personnel (three attorneys, one paralegal, and one IT employee) had access to the laptops at points during the relevant time period.

You asked whether Secretary Clinton's @clintonemail.com e-mails for the time period January 21, 2009 through February 1, 2013 were transferred or migrated to the hrcoffice.com account. As we indicated, Secretary Clinton did not transfer her @clintonemail.com e-mails for the time period January 21, 2009 through February 1, 2013 to her @hrcoffice.com account, nor did she instruct anyone to do so.

Sincerely,

  
David E. Kendall

[REDACTED] -144

b3 per  
b7E FBI

HRC-895

2/26/16  
Serial 145

b6 per  
b7C FBI

HRC-896

WILLIAMS & CONNOLLY LLP

725 TWELFTH STREET, N.W.

WASHINGTON, D. C. 20005-5901

(202) 434-5000

FAX (202) 434-5029

DAVID E. KENDALL  
(202) 434-5145  
dkendall@wc.com

EDWARD BENNETT WILLIAMS (1920-1988)  
PAUL R. CONNOLLY (1922-1978)

February 22, 2016

BY E-MAIL

[REDACTED]  
U.S. Department of Justice  
National Security Division  
950 Pennsylvania Avenue NW  
Washington, DC 20530

b6 per  
b7C FBI

Dear [REDACTED]

b6 per  
b7C FBI

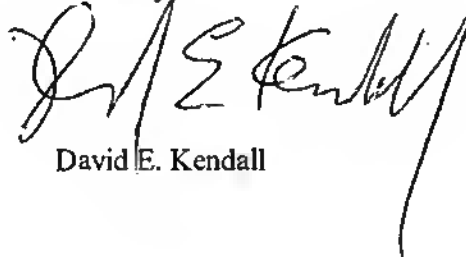
I write in response to your February 9, 2016 letter concerning certain equipment and devices. Following the inquiries that we have made in response to the requests in your letter, I can report the following.

In relation to your request regarding "Desktop computer in Whitehaven residence: model unknown (located at residence as of July 2010)," we have identified an iMac G5, 20" iSight computer that is believed to have been housed at the Whitehaven residence during 2010.

In relation to your request regarding an iPad "Generation 1 (Model A1337): Serial unknown (first use: June 2010)," we note that the iPad that we have previously identified to you, and which will be voluntarily produced pursuant to a consent letter is a Model A1337.

We have not located any equipment or devices matching the descriptions of the remaining items in your letter.

Sincerely,



David E. Kendall

HRC-897

b3 per  
b7E FBI





2/20/11  
Serial 146

b6 per  
b7C FBI

HRC-898

LAW OFFICES  
**WILLIAMS & CONNOLLY LLP**

725 TWELFTH STREET, N.W.  
WASHINGTON, D. C. 20005-5901  
(202) 434-5000  
FAX (202) 434-5029

DAVID E. KENDALL  
(202) 434-5145  
dkendall@wc.com

EDWARD BENNETT WILLIAMS (1920-1988)  
PAUL R. CONNOLLY (1922-1978)

February 23, 2016

BY E-MAIL

[REDACTED]  
U.S. Department of Justice  
National Security Division  
950 Pennsylvania Avenue NW  
Washington, DC 20530

Dear [REDACTED]

b6 per  
b7C FBI

This letter provides consent, in connection with the Department of Justice's security inquiry and subject to the provisions set forth herein, (1) to search the iPad, Model A1337 (hereinafter "the device") provided to the Federal Bureau of Investigation (FBI) for Secretary Clinton's e-mails and files dated January 21, 2009 to February 1, 2013; and (2) to conduct a forensic analysis of the device for the purpose of identifying information relevant to the Department of Justice's security inquiry. This consent applies solely to the above-described e-mails and files of Secretary Clinton, and not to any of her e-mails and files outside of the date range or to the e-mails or files of any other individuals that reside on the device.

b6 per  
b7C FBI

You have confirmed that any searches of the device will be undertaken initially by a filter team, who will hold back from the investigative team any e-mails or files that may contain privileged information. You have further confirmed that the filter team will set aside any e-mails or files (including Contacts) that are associated with the @hrcoffice.com domain account or created after February 1, 2013; and that any e-mails or files associated with that domain account or created after February 1, 2013 will not be searched or reviewed by anyone, even by the filter team, or otherwise be used in connection with your security inquiry or for any other purpose, as those e-mails and files were not in existence during the relevant time period. In order to preserve the data on the device, we agreed, as of December 23, 2015, not to turn on the device or to otherwise modify the device prior to its production to the FBI.

In connection with the filter team's efforts to segregate from the investigative team any e-mails or files that may contain privileged information, I incorporate by reference my October 1, 2015 letter, which provides a list of individuals and entities with whom Secretary Clinton may have communicated in a privileged context, and my October 16, 2015 e-mail, which supplemented that list.

HRC-899

b3 per  
b7E FBI

WILLIAMS & CONNOLLY LLP

[Redacted]

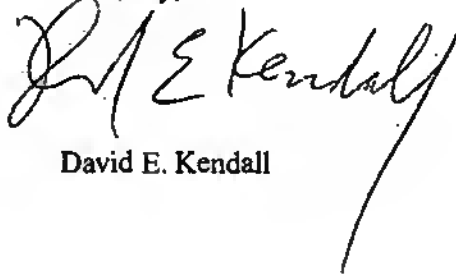
February 23, 2016

Page 2

b6 per  
b7C FBI

We request and anticipate that the device, as well as any of Secretary Clinton's non-federal record e-mails or files on the device, will be returned to us at the conclusion of your inquiry.

Sincerely,

A handwritten signature in black ink, appearing to read "D. E. Kendall", with a long, sweeping horizontal stroke extending to the right.

David E. Kendall

HRC-901

-1-

## FEDERAL BUREAU OF INVESTIGATION

b3 Per CIA  
b6 Per FBI, CIA  
b7C Per FBIDate of transcription 2/24/2016

On February 24, at approximately 3:50 PM, Special Agent [redacted] provided [redacted] [redacted] FBI liaison to the Counterespionage Group Counterintelligence Center, Central Intelligence Agency (CIA), with an LHM requesting assistance in contacting former CIA Deputy Director Michael Morell for an interview. The LHM was provided to [redacted] via the FBI Microsoft Lync system.

A copy of the LHM is enclosed in an accompanying IA.

Investigation on 2/24/2016 at Washington, DCb3 per FBI  
b7E per FBIFile # [redacted] - 147 Date dictated N/ABy SA [redacted]b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-902

2/26/16  
Serial 148

b6 per  
b7C FBI

HRC-903

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/24/2016

b3 per CIA  
b6 per FBI, CIA  
b7C per FBI

On February 24, 2016, SA [redacted] provided the Central Intelligence Agency (CIA) with an LHM to give notice that the FBI planned to use documents possibly containing classified CIA equities during future interviews. The LHM was provided to CIA detailee [redacted]

A copy of the LHM is enclosed in an attached 1A.

Investigation on 2/24/2016 at Washington, DC  
File # [redacted] - 148 Date dictated N/A

b3 per FBI  
b7E per FBI

By SA [redacted]

b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-904

3/1/16  
Serial 149

b6 per  
b7C FBI

HRC-905





United States Department of State

*Assistant Secretary of State  
for Diplomatic Security*

*Washington, D.C. 20520*

UNCLASSIFIED

February 26, 2016

TO: FBI – Peter Strzok

FROM: DS – Gregory B. Starr

SUBJECT: Request for Authority to use Classified Department of State  
Documents During Interviews

Thank you for your letter of February 12, 2016 regarding the FBI's request for authority to show classified Department of State e-mails and documents during interviews. We have received by e-mail a list of 74 individuals whom the FBI may want to interview regarding these documents.

The Department of State understands the FBI's desire to use these documents in interviews to pursue logical lines of questioning pursuant to your investigation, and similarly understands the desire to share these documents with both interviewees and their legal counsel if necessary. However, we are particularly concerned about sharing the 22 e-mails determined by the Intelligence Community (IC) to contain Top Secret (TS) information. The Department poses no objection to the FBI's plan to use the documents during interviews, but the Department believes that any individual, to include legal counsel, with whom these e-mails will be shared must have appropriate security clearances and must be read in to any special access program discussed in the relevant e-mail by the Department of State's Bureau of Intelligence and Research or by the appropriate IC element.

The Department has independently identified the recipients of the 22 TS e-mails for the purposes of placing the documents under proper controls and performing any necessary inadvertent disclosure procedures (the number of contemporaneous recipients is a small fraction of the list provided to the Department by the FBI). We have also compiled and can provide information on which recipients were cleared for access to the information at the time the e-mails were sent and which recipients are cleared for such access now. In addition, we can provide their current employment status and the status of their security clearance. We can provide the same information for those individuals on the FBI's

UNCLASSIFIED

HRC-906

b3 per  
b7E FBI

UNCLASSIFIED

- 2 -

list who did not have access to the e-mails determined by the IC to contain TS information. With respect to individuals not currently employed by the Department of State, the Department defers to the FBI to determine whether they may be granted a TS security clearance and have the necessary need to know for purposes of granting access to the information contained within the e-mails. If the FBI makes an affirmative determination, the Department has no objection to the e-mails being shown to the interviewees and their legal counsel.

Should you wish the Department of State to provide the information above, I request the FBI inform the Department of State in writing. We will then provide the requested information through our previously established channels.

Attachment:

Tab – FBI Letter dated February 12, 2016

UNCLASSIFIED

HRC-907

Approved: DS – Gregory B. Starr

Drafted: DS -

b6 per DOS, FBI  
b7C per DOS, FBI

Cleared: M – PKennedy (ok)  
L –  (ok)  
INR  (ok)  
INR  (ok)

3/1/16  
Serial 150

b6 per  
b7C FBI

HRC-909



United States Department of State

Assistant Secretary of State  
for Diplomatic Security

Washington, D.C. 20520

SENSITIVE BUT UNCLASSIFIED

March 1, 2016

**MEMORANDUM FOR RECORD TO THE FEDERAL BUREAU OF  
INVESTIGATION**

FROM: DS -Gregory B. Starr

SUBJECT: State's Compliance Regarding FBI Requests

(U) I am writing to follow up on our January 29<sup>th</sup> video teleconference and our February 1<sup>st</sup> meeting regarding the Department of State's response to the FBI investigation of Secretary of State Hillary R. Clinton's emails.

~~(SBU)~~ In our discussions on the production of records, the Department of State previously outlined current IT data management. As we have said, technical limitations affect our ability to achieve full compliance with the Bureau's request. We remain committed to working with the FBI investigative team to refine the request to ensure the most compliant response possible.

(U) My staff, with principal point of contact  can work with FBI personnel and offices from State to determine how or if we can be best responsive.

b6 per  
b7C DOS

Attachment:

Tab - DOS IT Technical Limitations

SENSITIVE BUT UNCLASSIFIED

HRC-910

Approved: S/ES - Joe Macmanus ( OK )

Drafted: DS - [REDACTED]

b6 per DOS, FBI  
b7C per DOS, FBI

Cleared: IRM - [REDACTED] (OK)  
INR - [REDACTED] (OK)  
A/GIS - Peggy Grafeld ( OK )  
S/ES - IRM [REDACTED] (OK)

~~**SENSITIVE BUT UNCLASSIFIED**~~

**Department of State IT Technical Limitations**

This paper outlines technical limitations of the Department of State's IT infrastructure as related to the FBI investigation into Secretary of State Hillary R. Clinton's emails.

**Limitations Due to Organization and Infrastructure**

(U) The Department of State (DOS) is committed to a thorough and timely response to the multiple data production requests from the Federal Bureau of Investigation (FBI). However, as previously noted, technical limitations affect this outcome. The Department's use of multiple networks, multiple administrative entities, and multiple policies governing the storage, retention, and disposition of documents and e-mails created over the time period outlined in the FBI's requests are the chief obstacle in our efforts to comply. In addition, until 2009 the Department's email retention policy relied on individual employees to print and file the emails the individual employee judged to be a record. Beginning in 2009, while "print and file" remained the official general guidance of the Department, the Department nevertheless captured the inboxes of certain senior officials on their departure. Again, as previously described, this capture would include all emails still residing in their email inbox but would not include any emails they had previously deleted.

**The Disparate Nature of Networks Create Challenges**

(SBU) Data requested by the FBI potentially resides on four different physical networks: OpenNet (unclassified up to SBU), PACE (unclassified for Public Affairs), ClassNet (up to Secret), and a TS/SCI information system operated by the Bureau of Intelligence and Research (INR). The Department does not maintain a single data owner or custodian for the OpenNet and ClassNet systems. Rather the data custodians, data owners, and official archivists vary according to which information resource management office supports the employee's bureau. Consequently, multiple offices may need to take action in response to the data production requests, depending on the assignment history of the employee in question. On these two networks, the IRM Bureau is the largest data custodian, managing approximately 25% of mailboxes, primarily for users located in the Washington DC region. Mailboxes for these users are limited to 5GB and users routinely use Personal Archives (.pst files) to store older e-mail that exceeds this storage location. These .pst files are stored in multiple locations by users, including home directories, other network shares, local workstations, and sometimes on removable media. As a result, IRM can only fully verify content of "active" mailboxes - anything archived in a .pst file may or may not be discovered. The

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~SENSITIVE BUT UNCLASSIFIED~~

data owner of these IRM-managed mailboxes is the bureau to which the employee is assigned. When the employee departs the Department, the data owner is responsible to determine the disposition of the mailbox and other user-created files. The data owner has the ability to retain the files within the bureau or transfer them to the A Bureau for official archiving. Regardless of the decision, the e-mail and files are removed from the on-line system six months after the employee leaves the Department. After this time, IRM can no longer access and provide the data.

~~(SBU)~~ The Secretary, other Department Principals, certain Special Envoys, their staffs, and the Executive Secretariat (S/ES) use OpenNet and ClassNet accounts in a system called the Principal Officers' Executive Management Support, or POEMS. The Executive Secretariat manages POEMS through its IT office, S/ES-IRM. When an official leaves the Department, S/ES-IRM, in coordination with record-keeping officials in S/ES and staff from the official's office, creates one or more .pst files containing the departing official's email, and saves all material stored on the official's personal drive, or P drive, to the same .pst. That data is backed up and kept indefinitely. S/ES-IRM performed this procedure for several prior administrations. While comprehensive in capturing all extant emails, this process did not, however, preserve emails previously deleted by the official.

(U) For overseas users and for domestic locations including the U.S. Mission to the UN, the Department's administrative center in Charleston, SC, the offices of the Inspector General, and U.S. passport offices, the data custodian and owner are the U.S. embassy or consulate where the employee works, or domestic office itself.

(U) Many Department employees including Foreign Service regularly rotate assignments from domestic to foreign assignments and between different locations in the Department. Department administrative restrictions place limits on the total bandwidth available for the storage of an individual employee's email and other data. Employees must therefore reduce their total on-line data storage prior to departure. In this way, they may enable the transfer of their data over the OpenNet and ClassNet networks from the office they are departing and to the office or mission abroad where they will arrive.

(U) Furthermore data transfer is also limited by policy. The Foreign Affairs Manual states, "Department workforce members must not take official files with them when they are reassigned to the field from the Department, to the Department from the field, or between posts unless the records transfer has been approved by A/GIS/IPS/RA." (5 FAM 432.4) As a result, finding specifically requested

~~SENSITIVE BUT UNCLASSIFIED~~



SENSITIVE BUT UNCLASSIFIED

for individuals who have rotated assignments since the date the item was created is especially difficult.

INR Network

(SBU) The Department's TS/SCI network is the most straightforward, particularly with respect to email, because there is only one data custodian (INR) for email sent on that network (sometimes referred to as "ice-mail" because it resolves to @state.ic.gov email addresses). Pursuant to Intelligence Community (IC) guidance, INR saves electronic records for 25 years. Since early 2014 it has backed records up to disk in addition to less reliable tapes, which previously were used exclusively. Also, in November 2014 INR installed CommVault Indexer. INR is now able to search electronic records, including ICEmail, relatively easily. For periods predating early 2014, however, restoration of email accounts may be difficult or, in the case of certain older accounts, impracticable if not impossible.

(SBU) Department users with ice-mail accounts fall into two categories: those who have "INR" (INR Information Support System) accounts and those with "eIntel" accounts. Each were first introduced to the Department by INR in 2008. During 2009-2013, INR maintained two mail servers, one for INRISS account holders and another for eIntel account holders. In early 2014 INR began transitioning eIntel users to the INRISS mail server. In the process of migration, only active accounts were migrated. If at the time it was reached in the migration process an account had not been logged into within the prior 365 days it was deemed inactive and retired; its mailbox contents were saved into a PST file and stored on a file server that was decommissioned in late 2014. That server is still available, and the PST files on this server can be accessed, but the PST files represent the user's mailbox as it existed the day the account was retired. To determine what the account looked like prior to its retirement INR must turn to the former eIntel mail server's tape backups, which are old and rely on infrastructure that is no longer in operation.

(SBU) With respect to the ICEmail accounts requested by the FBI, all were eIntel accounts and were inactive at the time of the 2014 migration mentioned above. With one exception, the associated PST files that were saved and stored contained no data, indicating a mailbox that was empty at the time of the migration. The one PST file that was not empty was copied and provided to the FBI.

SENSITIVE BUT UNCLASSIFIED

~~SENSITIVE BUT UNCLASSIFIED~~

**Detail Specific Search Requests Yield Better Results**

(U) The Department of State's current search technology does not allow cross-enclave searches. Most Department email data searches are done using relatively simple Outlook search tools, i.e. keyword searches of specific .psts or email boxes. Such searches are based within specific selected employees' records. It is therefore not possible to conduct a search in response to vague or general requests that specify "all e-mail to or from" or "all e-mail related to" a particular topic. Even within one of the above systems, there is no comprehensive search method that can even attempt such a search, much less provide accurate results. Instead requests should specify the employees' electronic records to be searched, timeframes, and relevant keywords. For example, "all e-mail between users *x* and *y* regarding (topic keywords)" or "all e-mail related to *w* either sent or received by users *x*, *y*, and *z* between *xxx* date and *yyy* date" will have a much greater chance of yielding responsive records, assuming those employees' records are available.

~~SENSITIVE BUT UNCLASSIFIED~~

3/18/16  
Serial 152

b6 per  
b7C FBI

HRC-919



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

March 8, 2016

Gregory B. Starr  
Assistant Secretary of State for Diplomatic Security  
U.S. Department of State  
2201 C Street, NW  
Washington, DC 20520

Dear Mr. Starr:

I am writing in response to your letter dated February 8, 2016 regarding the Department of State's Freedom of Information Act (FOIA) review of former Secretary of State Hillary Clinton's emails. We appreciate your concerns about the impact that the Department of State (DOS) actions may have on our ongoing investigation. Consistent with DOS's normal practice, as described in your letter, DOS should hold in abeyance any administrative action related to the mishandling of classified information for a limited and reasonable amount of time until the FBI can determine what, if any, impact such action might have on our investigation.

As for the emails that have been classified by the US Intelligence Community or DOS, the FBI recommends that you follow the standard security procedures established by DOS to remove potentially classified materials from any unclassified network.

Finally, with regard to Congressional requests for copies of the former Secretary's classified emails, the FBI defers to DOS to respond consistent with its normal practices.

Sincerely,

E.W. Priestap  
Assistant Director

HRC-920

3/18/66  
serial 153

b6 per  
b7C FBI

HRC-921

UNCLASSIFIED//~~FOUO~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-02-2019 BY C66W46B11 NSICG

Central Intelligence Agency



Washington, D.C. 20505

MAR 01 2016

b6 per FBI  
b7C per FBI

MEMORANDUM FOR: Director  
Federal Bureau of Investigation

ATTENTION: Peter P. Strzok  
Section Chief, CD-4  
Counterintelligence Division

SUBJECT: (U//~~FOUO~~) MIDYEAR EXAM - Response to LHM

REFERENCE: (U//~~FOUO~~) FBI LHM, dtd 24 Feb 2016

Assign to MYE  
Special SA  
[Redacted]

[Redacted]  
3/7/16

1. (U//~~FOUO~~) Action Requested: For your information and action, as appropriate. Please forward to Special Agent [Redacted]

b6 per FBI  
b7C per FBI

2. (U//~~FOUO~~) The following information is provided for the exclusive use of your organization for background, investigative, or lead purposes, as appropriate. It may not be used in any legal proceeding without prior coordination. While the information may be shared with necessary investigative components of your organization, it should not be released in any form to other components within the CIA or any other agencies without prior approval of the Chief, Counterintelligence Mission Center, [Redacted] Counterespionage Group (C/CIMC/[Redacted]/CEG). Details contained in this CIOL may not be uploaded into any SIPRNET-based computer system.

b3 Per CIA

CIOL-0183-16

HRC-922

UNCLASSIFIED//~~FOUO~~

b3 per FBI  
b7E per FBI

SUBJECT: (U//~~FOUO~~) MIDYEAR EXAM - Response to LHM

3. (U//~~FOUO~~) This CIOL responds to your LHM dated 24 February 2016 in which you asked for CIA assistance in arranging an FBI interview of former DDCIA Michael Morell on a voluntary basis. FBI detailee to CIMC/CEG further explained that FBI is seeking this interview because of Mr. Morell's subject matter expertise; he is not the target or subject of the underlying sensitive matter. Mr. Morell requests that his attorney, Ken Wainstein, be present at the interview; Mr. Wainstein is unable to meet on 4 March 2016. Mr. Morell indicated that Mr. Wainstein can be reached at (202) 862-2474 to schedule a meeting.

4. (U//~~FOUO~~) Please address all correspondence concerning this matter to the Counterintelligence Mission Center, [redacted] b3 Per CIA  
[redacted] Counterespionage Group, Attention: [redacted] b6 Per CIA  
commercial line [redacted] referencing the CIOL number [redacted] b7C Per CIA  
given below.

FOR THE ASSISTANT DIRECTOR/CIA FOR COUNTERINTELLIGENCE:



b3 Per CIA  
b6 Per CIA  
b7C Per CIA

CIOL-0183-16

4/1/86  
Serial 154

b6 per  
b7C FBI

HRC-924





United States Department of State


Assistant Secretary of State  
for Diplomatic Security

Washington, D.C. 20520

UNCLASSIFIED

March 21, 2016

TO: FBI – E.W. Priestap

FROM: DS – Gregory B. Starr 

SUBJECT: Congressional Review of Hillary Clinton E-mails Classified Secret or

Thank you for the letter of March 8, 2016 (Tab 1), which contained helpful guidance. I am writing to inform you that the Department of State intends to make available, with limited redactions, versions of the Hillary Clinton e-mails classified in excess of Confidential during the Freedom of Information Act review process to cleared members and staff of the Senate Foreign Relations Committee (SFRC) possibly starting as early as this week. The e-mails may be shared with additional committees in the future. The e-mails will be available for review, either *in-camera* or at the State Department, but will not be retained by the reviewers. In addition, reviewers will not be permitted to make copies or otherwise reproduce the contents of the e-mails during their scheduled review.

The 22 e-mails determined by the IC to contain Top Secret information will not be made available to the SFRC.

Attachments:

Tab 1 – FBI letter dated March 8, 2016

Tab 2 – Department of State letter dated February 8, 2016

UNCLASSIFIED

HRC-925

Approved: DS/FO - [redacted]

b6 per DOS, FBI  
b7C per DOS, FBI

Drafted: DS/FO - [redacted]

Cleared:	M -	[redacted]	(ok)
	L -	[redacted]	(ok)
	L/M/DS -	[redacted]	(ok)
	INR -	[redacted]	(ok)
	A/GIS -	[redacted]	(ok)
	H -	[redacted]	(ok)
	DS/Leg -	[redacted]	(ok)



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

March 8, 2016

Gregory B. Starr  
Assistant Secretary of State for Diplomatic Security  
U.S. Department of State  
2201 C Street, NW  
Washington, DC 20520

Dear Mr. Starr:

I am writing in response to your letter dated February 8, 2016 regarding the Department of State's Freedom of Information Act (FOIA) review of former Secretary of State Hillary Clinton's emails. We appreciate your concerns about the impact that the Department of State (DOS) actions may have on our ongoing investigation. Consistent with DOS's normal practice, as described in your letter, DOS should hold in abeyance any administrative action related to the mishandling of classified information for a limited and reasonable amount of time until the FBI can determine what, if any, impact such action might have on our investigation.

As for the emails that have been classified by the US Intelligence Community or DOS, the FBI recommends that you follow the standard security procedures established by DOS to remove potentially classified materials from any unclassified network.

Finally, with regard to Congressional requests for copies of the former Secretary's classified emails, the FBI defers to DOS to respond consistent with its normal practices.

Sincerely,

A handwritten signature in dark ink, appearing to read "E.W. Priestap", is written over the typed name.

E.W. Priestap  
Assistant Director



**United States Department of State**

*Assistant Secretary of State  
for Diplomatic Security*

*Washington, D.C. 20520*

UNCLASSIFIED

February 8, 2016

TO: FBI – E.W. Priestap

FROM: DS – Gregory B. Starr

A handwritten signature in black ink, appearing to read "Gregory B. Starr", written over the printed name.

SUBJECT: Department of State Hillary Clinton E-mail Review

I am writing to follow up on our January 29, 2016 video teleconference regarding the current status of the Department of State's Freedom of Information Act (FOIA) reviews of former Secretary of State Hillary R. Clinton's e-mails.

Late last week the Department reported that 22 Clinton e-mails would not be publically released due to their Top Secret (TS) classification at the request of the Intelligence Community (IC). That is, under FOIA, these e-mails were denied in full, but they are being accounted for in the Clinton e-mail collection. In addition to these 22 TS e-mails, portions of 22 other e-mails have been classified Secret by the State Department or the IC to date. Finally, approximately 1300 e-mails contain sensitive information that was previously redacted and classified as Confidential prior to the e-mails' release under our FOIA process.

The Department of State is prepared to take appropriate administrative action for any instances of mishandling of classified information in accordance with our own internal processes (see Attachment). However, we appreciate the sensitivity of ongoing criminal investigations generally and do not want to compromise or hinder the FBI's current investigation in any way. It has been the normal practice of the Department and the Bureau of Diplomatic Security to delay taking administrative action against current State employees when active criminal investigations of a parallel nature are underway. I request the Department of Justice (DOJ) and FBI inform the Department of State in writing as soon as possible if the Department of State can under administrative investigations or inquiries into possible security violations, or if the Department of State should delay due to the current criminal investigation until notification to proceed is received from the DOJ and FBI.

In addition, following up on my letter of September 15, 2015, please be advised that pending further guidance from the FBI we are still – as a general rule – not removing any emails that have since been classified from any unclassified systems or providing instruction to individuals that may have upgraded classified emails on non-official email accounts to take steps to protect this information.

Finally, Congressional Committees have requested unredacted copies of former Secretary Clinton's classified e-mails. I request DOJ and FBI inform the Department of State in writing as soon as possible as to whether they have any concerns regarding such a possible production of these e-mails in unredacted form at this juncture. I note that we are not considering turning over to any Committee documents the members/staff are not cleared to receive because of their classification level.

Attachment:

Tab – 12 FAM 550 Security Incident Program

Approved: DS – Gregory B. Starr

Drafted: DS -

b6 per DOS, FBI  
b7C per DOS, FBI

Cleared: L -  (ck)

~~SECRET~~

HRC-931

~~SECRET~~

~~SECRET//NOFORN~~**FEDERAL BUREAU OF INVESTIGATION****Collected Item Log**

(U) Event Title: ~~(S)~~ Collect from DoS under  
banner/FOIA authority

Date: 04/06/2016

Approved By: [REDACTED]

b6 per FBI  
b7C per FBI

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U) ~~(S//NF)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3 per FBI  
b7E per FBI

Reason: 1.4(c)  
Derived From: Multiple  
Sources  
Declassify On: 20411231

Full Investigation Initiated: 07/10/2015

Collected From: [REDACTED]

Department of State

b6 per DOS  
b7C per DOS

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Details: No Details Provided

**Item Type**

1B Digital

**Description**

(U) ~~(S)~~ DVD containing PST for [REDACTED]  
Collected On: 04/06/2016  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: N/A  
Specific Location: N/A  
Device Type: Compact Disc/Digital Video  
Disc(CDs/DVDs)  
Number of Devices Collected: 1

b6 per DOS, FBI  
b7C per DOS, FBI~~SECRET//NOFORN~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-932



~~SECRET//NOFORN~~

(U)


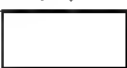

Title: ~~(S)~~ Collect from DoS under banner/FOIA authority

Re:  04/06/2016

b3 per  
b7E FBI

♦♦

~~SECRET//NOFORN~~

 -157  
4/6/2016 4/11/16  
 

~~SECRET~~

b3  
b6  
b7C per  
b7E FBI

HRC-936

~~SECRET~~

~~SECRET//NOFORN~~



**U.S. Department of Justice**  
**Federal Bureau of Investigation**  
Washington, D.C. 20535-0001

Date: March 18, 2016

To: [REDACTED]  
Counterespionage Group  
Counterintelligence Center CIA

b3 Per CIA  
b6 Per CIA  
b7C Per CIA

From: Peter P. Strzok  
Section Chief  
Counterespionage Section

Subject: Request for Identification

~~(S//NF)~~ The FBI Washington Field Office (WFO) respectfully requests the CIA's assistance in identifying the names and current location of the individuals who occupied the positions listed below during the date ranges provided. This assistance is in regards to requests for FBI interviews. These interviews are voluntary and pertain to a sensitive matter in which the FBI believes the individuals may be of assistance.

b1 Per CIA  
b3 Per CIA

- [REDACTED] May 2011 - September 2012 (S)
- [REDACTED] May 2011 - September 2012
- [REDACTED] May 2011 - September 2012 (S)
- [REDACTED] May 2011 - September 2012
- Director, Counterterrorism Center, 2010 - 2012
- [REDACTED] 2010 - 2012 (S)

~~SECRET//NOFORN~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-937

~~SECRET//NOFORN~~

(U//~~FOUO~~) If you have any questions regarding this request,  
please direct all inquiries to Special Agent [redacted] at  
[redacted]

b6 per  
b7C FBI

Sincerely,

Peter P. Strzok  
Section Chief  
Counterespionage Section

♦♦

~~SECRET//NOFORN~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-938

[redacted] -158  
4/13/16 4/11/16  
[redacted] [redacted]

~~SECRET~~

b3  
b6  
b7C per  
b7E FBI

HRC-939

~~SECRET~~

~~SECRET~~ [ ] ~~NOFORN~~

b3 Per CIA

Central Intelligence Agency



Washington, D.C. 20505

APR 07 2016

MEMORANDUM FOR: Director  
Federal Bureau of Investigation

ATTENTION: Peter P. Strzok, II  
Section Chief, CD-4  
Counterintelligence Division

SUBJECT: (U) ~~(S//NF)~~ MIDYEAR EXAM - Response to LHM

REFERENCE: (U//~~FOUO~~) FBI LHM, dtd 16 March 2016

1. (U//~~FOUO~~) Action Requested: For your information and action, as appropriate. Please forward to Special Agent [ ]

b6 per  
b7C FBI

2. (U//~~FOUO~~) The following information is provided for the exclusive use of your organization for background, investigative, or lead purposes, as appropriate. It may not be used in any legal proceeding without prior coordination. While the information may be shared with necessary investigative



CIOL-0254-16

b3 Per CIA

~~SECRET~~ [ ] ~~NOFORN~~

HRC-940

(U) SUBJECT: ~~(TS//NF)~~ MIDYEAR EXAM - Response to LHM

components of your organization, it should not be [ ]ased in any form to other components within the CIA or any other agencies without prior approval of the Chief, Counterintelligence Mission Center, [ ] Counterespionage Group (C/CIMC/[ ] CEG). Details contained in this CIOL may not be uploaded into any SIPRNET-based computer system.

b3 Per CIA

3. ~~(S//NF)~~ Per the referenced FBI Letterhead Memorandum (LHM) dated 16 March 2016, CIA provides the attached spreadsheet [ ]

b1 Per CIA

b3 Per CIA

b6 Per CIA

(S)

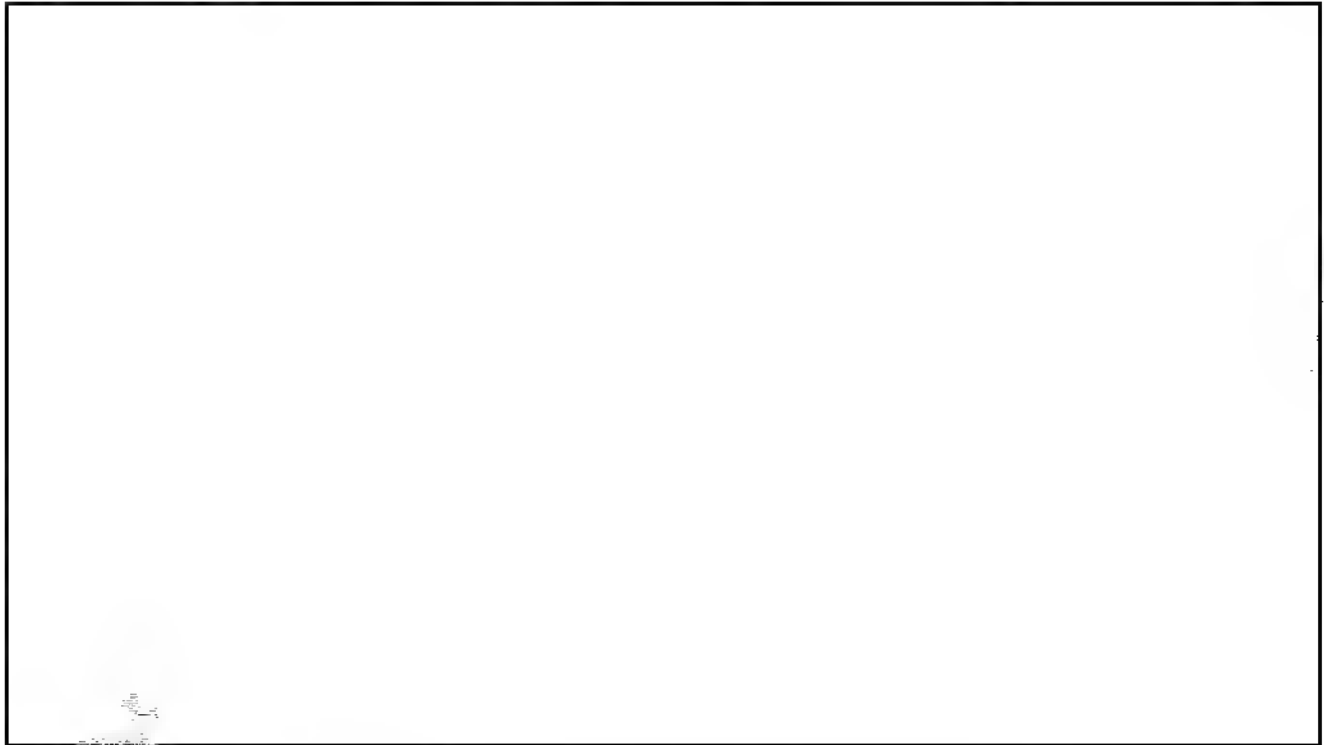
~~SECRET~~

~~NOFORN~~

b3 Per CIA

(U) SUBJECT: ~~(S//NF)~~ MIDYEAR EXAM - Response to LHM

b1 Per CIA  
b3 Per CIA  
b6 Per CIA



(S)

3. (U//~~FOUO~~) Please address all correspondence concerning this matter to the Counterintelligence Mission Center, [redacted] Counterespionage Group, Attention: [redacted] commercial line [redacted] referencing the CIOL number given below.

b3 Per CIA

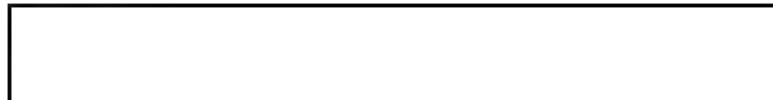
FOR THE ASSISTANT DIRECTOR/CIA FOR COUNTERINTELLIGENCE:



b3 Per CIA  
b6 Per CIA

CIOL-0254-16

Attachment: (S//~~NF~~)



(S) b1 Per CIA  
b3 Per CIA

~~SECRET~~

~~NOFORN~~

b3 Per CIA



[redacted] - 162  
4/18/2016 5/2/16  
[redacted]

b3  
b6  
b7C per  
b7E FBI

HRC-959

LAW OFFICES  
**WILLIAMS & CONNOLLY LLP**  
725 TWELFTH STREET, N.W.

DAVID E. KENDALL  
(202) 434-5145  
dkendall@wc.com

WASHINGTON, D. C. 20005-5901  
(202) 434-5000  
FAX (202) 434-5029

EDWARD BENNETT WILLIAMS (1930-1986)  
PAUL R. CONNOLLY (1922-1975)

April 15, 2016

BY E-MAIL

[REDACTED]  
U.S. Department of Justice  
National Security Division  
950 Pennsylvania Avenue NW  
Washington, DC 20530

b6 per  
b7C FBI

Dear [REDACTED]

b6 per  
b7C FBI

This letter provides consent, in connection with the Department of Justice's security inquiry and subject to the provisions set forth herein, to conduct a preliminary examination of the iPad mini, Model A1432 (hereinafter "the device") provided to the Federal Bureau of Investigation (FBI), for the limited purposes of (1) determining whether any of Secretary Clinton's e-mails and files dated January 21, 2009 to February 1, 2013 reside on the device; and (2) conducting an analysis of the device to determine whether any intrusions occurred. You have represented to us that the intrusion analysis will not involve search or review of any e-mails or files that reside on the device. Furthermore, to the extent the FBI determines in that preliminary examination that no e-mails or files of Secretary Clinton dated January 21, 2009 to February 1, 2013 reside on the device, you have agreed to return the device to us promptly without conducting any further examination of the device other than the intrusion analysis.

To the extent the FBI determines in its preliminary examination that e-mails or files of Secretary Clinton dated January 21, 2009 to February 1, 2013 do reside on the device, this letter provides consent, in connection with the Department of Justice's security inquiry and subject to the provisions set forth herein, to search such e-mails and files of Secretary Clinton dated January 21, 2009 to February 1, 2013 (in accordance with the procedures outlined below) for the purpose of identifying information relevant to the Department of Justice's security inquiry. This consent applies solely to the above-described e-mails and files of Secretary Clinton (to the extent any such files exist on the device), and not to any of her e-mails and files outside of the date range or to the e-mails or files of any other individuals that may reside on the device.

April 15, 2016

Page 2

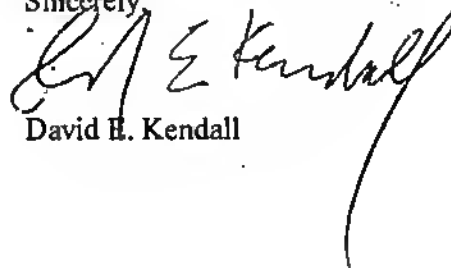
b6 per  
b7C FBI

You have confirmed that the searches consented to above will be undertaken first by a filter team, who will hold back from the investigative team any e-mails or files that may contain privileged information, as well as all e-mails and files outside of the scope of the searches consented to above. You have further confirmed that the filter team will set aside any e-mails or files (including Contacts) that are associated with the @hrcoffice.com domain account or were created after February 1, 2013; and that any e-mails or files associated with that domain account or created after February 1, 2013 will not be searched or reviewed by anyone, even by the filter team, or otherwise be used in connection with your security inquiry or for any other purpose, as those e-mails and files were not in existence during the relevant time period.




In connection with the filter team's efforts to segregate from the investigative team any e-mails or files that may contain privileged information, I incorporate by reference my October 1, 2015 letter, which provides a list of individuals and entities with whom Secretary Clinton may have communicated in a privileged context, and my October 16, 2015 e-mail, which supplemented that list.

In the event that the device is determined in the FBI's preliminary examination to contain e-mails or files of Secretary Clinton dated January 21, 2009 to February 1, 2013, we request and anticipate that the device, as well as any of Secretary Clinton's non-federal record e-mails or files on the device, will be returned to us at the conclusion of your inquiry.

Sincerely,



David H. Kendall

 -163  
4/26/2016   


b3  
b6  
b7C per  
b7E FBI

HRC-962

LAW OFFICES  
**WILLIAMS & CONNOLLY LLP**  
725 TWELFTH STREET, N.W.

DAVID E. KENDALL  
(202) 434-5145  
dkendall@wc.com

WASHINGTON, D. C. 20005-5901

(202) 434-5000

FAX (202) 434-5029

EDWARD BENNETT WILLIAMS (1920-1988)  
PAUL R. CONNOLLY (1922-1978)

April 22, 2016

BY E-MAIL

[REDACTED]  
U.S. Department of Justice  
National Security Division  
950 Pennsylvania Avenue NW  
Washington, DC 20530

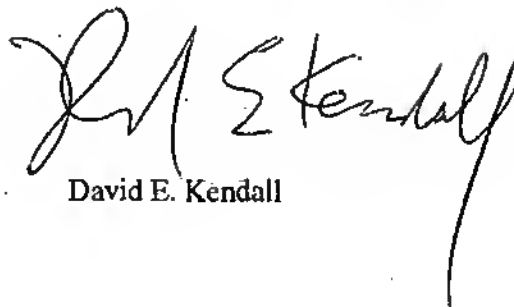
Dear [REDACTED]

b6 per  
b7C FBI

b6 per  
b7C FBI

This letter confirms that, pursuant to our discussions, Williams & Connolly LLP ("W&C") has provided to the Department of Justice two W&C hard drives (a Samsung Lenovo 256 GB hard drive and a Samsung Lenovo 128 GB hard drive) (the "drives") for the sole purpose of destruction. The drives each contained a copy of data that W&C had previously provided to the Department of Justice, as well as other W&C attorney-client privileged and attorney work product materials. Pursuant to our agreement, W&C has deleted all data from the drives prior to providing them to the Department. We understand that once the drives have been destroyed, you will provide us confirmation of that fact. For avoidance of doubt, this letter does not provide any consent to search the drives prior to their destruction.

Sincerely,

  
David E. Kendall

HRC-963

5/21/16  
Serial 166

b6 per  
b7C FBI

HRC-975



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

David E. Kendall, Esq.  
Katherine M. Turner, Esq.  
Williams & Connolly LLP  
725 Twelfth Street, N.W.  
Washington, DC 20005

February 9, 2016

Dear Mr. Kendall and Ms. Turner,

b5 per NSD

**1. Laptop Computer**

- MacBook Air: Serial unknown (purchased November 2008)

**2. Desktop Computer**

- Desktop computer in Whitehaven residence: model unknown (located at residence as of July 2010)

**3. iPads**

- Generation 1 (Model A1337): Serial unknown (first use: June 2010)
- Generation 3: Serial DLXHFT7VDVGJ (first use: May 2012)
- Mini: Serial unknown

**4. Phones Associated with (212) 920-6329**

- BlackBerry Curve 8310: IMEI 359315014408230 (January 2009 – May 2009)
- BlackBerry Curve 8900: IMEI 359485022135651 (June 2009 – September 2009)
- BlackBerry Curve 8900: IMEI 358453025219261 (September 2009 – August 2011)
- BlackBerry Curve 8900: IMEI 358453029684668 (August 2011 – February 2012)
- BlackBerry Curve 8900: IMEI 355383038220886 (February 2012)
- BlackBerry Bold 9900: IMEI 357966040796790 (February 2012)
- BlackBerry Curve 8900: IMEI 355383039952164 (February 2012 – March 2012)
- BlackBerry Curve 9360: IMEI 357965040112701 (February 2012 – March 2013)
- BlackBerry Curve 9360: IMEI 357965043386724 (March 2013 – October 2013)

HRC-976

- BlackBerry Bold 9900: IMEI 357966044557578 (October 2013 – November 2015)
- BlackBerry Bold 9900: IMEI 357966044869312 (December 2014)

**5. Phones Associated with (212) 920-7127**

- Sony Xperia Z C6603: IMEI 355762054150000 (April 2013)
- Motorola EX431G: IMEI 359486042036950 (September 2013 – February 2014)

**6. SIM Cards with One of the Following Identifiers**

**IMSI (stored digitally on the SIM card):**

- 310410088779408
- 310410248923744
- 310410492968953
- 310410758808198
- 310410774223342
- 310410785717450
- 310410178586207
- 310410208687757
- 310410248923744
- 310410283447343
- 310410331125794
- 310410408399442
- 310410676110393
- 310410785725002
- 310410614126238

**ICCID (may be written on outside of SIM card):**

- 89014104200887794085
- 89014102232489237447
- 89014104254929689530
- 89014103277588081989
- 89014103277857174507



b5 per NSD

Sincerely,



b6 per  
b7C FBI



6/30/16  
Serial 171

b6 per  
b7C FBI

HRC-987

[REDACTED] (RO) (FBI)

b6 per FBI  
b7C per FBI

From: [REDACTED] (NSD) [REDACTED]  
Sent: Friday, March 11, 2016 3:42 PM  
To: [REDACTED] (RO) (FBI)  
Cc: [REDACTED] (NSD) (JMD) [REDACTED] (CD) (FBI)  
Subject: iPad Minis

b5 per NSD  
b6 per FBI  
b7C per FBI

[REDACTED]

[REDACTED]

1. A1489/F9FMW65UFCM9
2. A1432/F4GJG37XF193

Thanks.

b6 per FBI  
b7C per FBI

National Security Division  
U.S. Department of Justice

[REDACTED]

HRC-988



Serial 172

~~SECRET~~

b3 per  
b7E FBI



HRC-989

~~SECRET~~

~~SECRET~~

## FEDERAL BUREAU OF INVESTIGATION

**Precedence:** ROUTINE

**Date:** 06/28/2016

**To:** Washington Field

**From:** Washington Field

CI-13

**Contact:** SOS

**Approved By:**

**Drafted By:**

**Case ID #:** ~~(S)~~

**Title:** (U) ~~(S)~~ MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED;  
UNKNOWN SUBJECT OR COUNTRY;  
SENSITIVE INVESTIGATIVE MATTER (SIM)

**Synopsis:** (U//~~FOUO~~) Documents details related to the investigation's inability to acquire 19 electronic devices potentially utilized to access the hdr22@clintonemail.com or hrod17@clintonemail.com e-mail accounts.

**Classified By:** F22M62K21

**Derived From:** FBI NSIC dated 20130301

**Declassify On:** 20411231

**References:**

Serial 36  
Serial 41  
Serial 42

### FEDERAL GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(E)

Do not disseminate except as authorized by federal rule of criminal procedure 6(e).

**Details:** (U//~~FOUO~~) During the course of its investigation, the Federal Bureau of Investigation (FBI) identified electronic devices with e-mail capability associated with former Secretary of State HILLARY RODHAM CLINTON through witness interviews, Grand Jury subpoena returns and information provided by CLINTON's defense counsel. As of the date of this communication, the FBI identified, but was unable to acquire, 19 devices which possibly were used to access CLINTON's hdr22@clintonemail.com or hrod17@clintonemail.com e-mail accounts.

~~SECRET~~

~~SECRET~~

## FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) Unless specifically noted, the FBI was unable to find explicit evidence indicating the devices outlined in this communication were connected to either the Bryan Pagliano or Platte River Networks (PRN) e-mail servers. However, the FBI was unable to identify all of the devices that accessed CLINTON's e-mail or synced with the servers due to the limitations of the data and log files available from the hardware collected.

(U)

[REDACTED]

b3  
b6  
b7C per  
b7E FBI

(U)

~~(S)~~ The author

[REDACTED]

[REDACTED]

b5 per NSD

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

b3  
b6 per  
b7C FBI

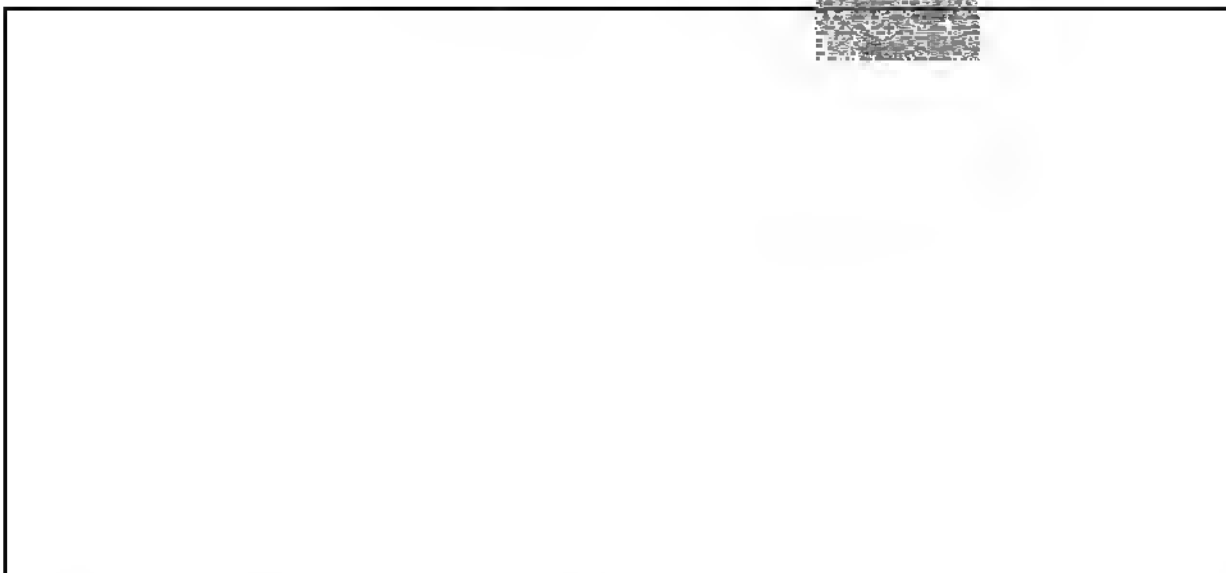
[REDACTED]

~~SECRET~~

~~SECRET~~

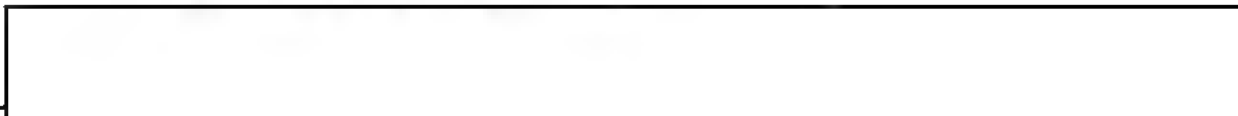
FEDERAL BUREAU OF INVESTIGATION

b3 per FBI  
b6 per FBI  
b7C per FBI



(U) Apple iPads (Two Identified)

b3 per FBI  
b5 per NSD  
b6 per FBI  
b7C per FBI  
b7E per FBI



b3 per FBI



~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b5 per NSD

(U) Laptop and Desktop Computers (Four Identified)

b5 per NSD

(U//~~FOUO~~) Finally, the FBI investigation identified an Apple MacBook Pro laptop computer which contained a full archive of the e-mails from CLINTON's tenure as Secretary of State. In March 2013, CLINTON's hdr22@clintonemail.com e-mail address was publicly released following the on-line posting of e-mail exchanges between CLINTON and an informal political advisor,

~~SECRET~~

~~SECRET~~

## FEDERAL BUREAU OF INVESTIGATION

SIDNEY BLUMENTHAL. According to interviews of COOPER and CLINTON aide MONICA HANLEY, the event prompted a switch to CLINTON's new e-mail account, hrod17@clintonemail.com, and the creation of an archive of CLINTON's State Department tenure e-mails. In late March 2013, HANLEY created an archive of the e-mails in CLINTON's account on an Apple MacBook Pro from HANLEY's New York residence. HANLEY subsequently shipped the laptop to PRN employee [REDACTED] in February 2014 to migrate the archive onto the PRN server. Following [REDACTED] migration, he shipped the laptop to [REDACTED] who was CLINTON's office manager at the time. [REDACTED] indicated she never received the laptop from [REDACTED] however, she advised that CLINTON's staff was moving offices at the time and it would have been easy for the package to get lost during the transition period. The FBI did not identify the location of the Apple MacBook Pro computer.

b6 per  
b7C FBI

~~SECRET~~



b3  
b6  
b7C per  
b7E FBI

7/6/2016  
7/6/2016

HRC-997

[REDACTED] (WF) (FBI)

b6 per FBI  
b7C per FBI

From: Turner, Katherine [KTurner@wc.com]  
Sent: Tuesday, July 05, 2016 10:14 PM  
To: [REDACTED] (NSD) (JMD); Kendall, David; [REDACTED]  
Cc: [REDACTED] (NSD) (JMD); [REDACTED] (USAVAE); [REDACTED] (USAVAE);  
[REDACTED] (WF) (FBI); [REDACTED] (WF) (FBI)  
Subject: RE: Attorney Notes

Thanks very much, [REDACTED] We will let Cheryl and Heather know.

b6 per FBI  
b7C per FBI

Sent with Good ([www.good.com](http://www.good.com))

From: [REDACTED] (NSD)  
Sent: Tuesday, July 05, 2016 10:11:44 PM  
To: Kendall, David; Turner, Katherine; [REDACTED]  
Cc: [REDACTED] (NSD); [REDACTED] (USAVAE); [REDACTED] (USAVAE); [REDACTED]  
[REDACTED] (WF) (FBI); [REDACTED] (WF) (FBI)  
Subject: Attorney Notes

b6 per FBI  
b7C per FBI

David/Katherine [REDACTED]

b5 per NSD  
b6 per FBI  
b7C per FBI

Thanks,  
[REDACTED]

b6 per FBI  
b7C per FBI

[REDACTED]  
Justice

National Security Division U.S. Department of

Phone: [REDACTED]

This message and any attachments are intended only for the addressee and may contain information that is privileged and confidential. If you have received this message in error, please do not read, use, copy, distribute, or disclose the contents of the message and any attachments. Instead, please delete the message and any attachments and notify the sender immediately. Thank you.

11/16  
Serial 825

b6 per  
b7C FBI

HRC-999



U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

DEC 29 2015

Special Agent [redacted]  
Federal Bureau of Investigations  
Washington Field Office  
601 4<sup>th</sup> Street N.W.  
Washington, DC 20535

b6 per  
b7C FBI

Re: Declination of Bryan M. Pagliano

Dear Special Agent [redacted]

b6 per  
b7C FBI

The Public Integrity Section has completed its review of allegations concerning Bryan M. Pagliano.

This letter will confirm that we have concluded that initiation of criminal proceedings in this matter is not warranted and we have declined prosecution. We understand that your office concurs with this decision.

If you have any questions regarding this matter, please call me or contact trial attorney

[redacted] at [redacted]

b6 per  
b7C DOJ-CRIM

Sincerely,

Raymond N. Hulser  
Chief  
Public Integrity Section

HRC-1000

3 per  
b7E FBI

Serial 172  
7/18/16

b6 per  
b7C FBI

MAN

Serial 172

EC from

re: 19 emails

[REDACTED] (WF) (FBI)

b6 per FBI  
b7C per FBI

From: [REDACTED] (WF) (FBI)  
Sent: Thursday, June 09, 2016 3:54 PM  
To: [REDACTED] (WF) (FBI)  
Subject: FW: iPad Minis

From: [REDACTED] (RO) (FBI)  
Sent: Monday, March 14, 2016 9:49 AM  
To: [REDACTED] (WF) (FBI)  
Subject: FW: iPad Minis

b6 per FBI  
b7C per FBI

From: [REDACTED] (NSD) [REDACTED]  
Sent: Friday, March 11, 2016 3:42 PM  
To: [REDACTED] (RO) (FBI)  
Cc: [REDACTED] (NSD) (JMD) [REDACTED] (CD) (FBI)  
Subject: iPad Minis

b6 per FBI  
b7C per FBI

b5 per NSD  
b6 per FBI  
b7C per FBI

1. A1489/F9FMW65UFCM9  
2. A1432/F4GJG37XF193

Thanks,  
[REDACTED]  
[REDACTED]

b6 per FBI  
b7C per FBI

National Security Division  
U.S. Department of Justice  
[REDACTED]

HRC-1006

[redacted] - 179  
7/22/2016 [redacted]  
[redacted] 7/22/16

b3  
b6  
b7C per  
b7E FBI

HRC-1007



**U.S. Department of Justice**

**National Security Division**

*Washington, D.C. 20530*

David E. Kendall, Esq.  
Williams & Connolly LLP  
725 Twelfth Street, N.W.  
Washington, DC 20005

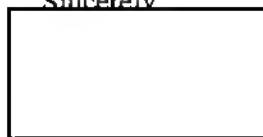
July 21, 2016

Dear Mr. Kendall,



b5 per NSD

Sincerely



b6 per  
b7C FBI

HRC-1008



7/22/16  
Serial 180

b6 per  
b7C FBI

HRC-1009

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/21/2016

b6 per DOS, FBI  
b7C per DOS, FBI

On July 21, 2016, Special Agent [redacted] provided [redacted] of the United States Department of State, Diplomatic Security Service, a package containing the following two (2) DVDs:

"Final Production to U.S. Department of State Disc 1; Datasets 1-3" Disc #DEHQ76

"Final Classification Determinations" Disc #DEHQ75

b6 Per  
b7C DOS

A copy of the FD-597 [Receipt for Property] signed by [redacted] acknowledging the receipt of said DVDs is enclosed in an accompanying 1A, along with a copy of Disc #DEHQ75

Investigation on 07/21/2016 at Washington, D.C.

b3 per FBI  
b7E per FBI

# [redacted] TS and [redacted] Date dictated N/A

By SA [redacted]

b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-1010

7/29/14  
Serial 181

b6 per  
b7C FBI

HRC-1011

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

**MEMORANDUM OF UNDERSTANDING**  
**Between the Federal Bureau of Investigation and the United States Department of State**  
**Governing Retrieved Materials**

**(U) INTRODUCTION**

1. (U//~~FOUO~~) This MEMORANDUM OF UNDERSTANDING ("MOU") between the Federal Bureau of Investigation ("FBI") and the United States Department of State ("DOS") (collectively, the "Parties") memorializes and confirms the Parties' agreement governing the status and handling of certain information provided by the FBI to DOS in furtherance of agency record determinations by DOS.

**(U) DEFINITIONS**

2. (U//~~FOUO~~) The "FBI's Investigation" means the FBI's investigation concerning a referral from the Inspector General of the Intelligence Community ("ICIG") in connection with former Secretary Hillary Clinton's use of a private e-mail server.
3. (U//~~FOUO~~) "Retrieved Materials" means certain information that the FBI has provided or that it may in the future provide to DOS for review and determination of DOS agency record status.

**(U) BACKGROUND**

4. (U//~~FOUO~~) During the course of the FBI's Investigation, the FBI obtained certain information that may include DOS agency records.
5. (U//~~FOUO~~) Pursuant to a July 8, 2016 request from DOS, the FBI notified DOS on July 12, 2016 that it would provide such information for review and DOS agency record determination pursuant to the Federal Records Act and for subsequent Freedom of Information Act (FOIA) processing as appropriate.

**(U) UNDERSTANDING AND AGREEMENT**

6. (U//~~FOUO~~) The purpose of this MOU is to express and embody the Parties' understanding and agreement regarding the conditions under which the FBI has provided the Retrieved Materials to DOS.
7. (U//~~FOUO~~) The Parties understand and agree that the Retrieved Materials are being provided to DOS for the purpose of conducting a review and determination of DOS agency record status.
  - a. (U//~~FOUO~~) During the review, upon DOS's determination that a document from the Retrieved Materials is a DOS agency record, custody of that document will immediately transfer to DOS. DOS may then process and use the identified DOS

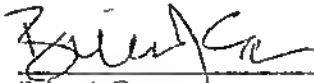
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

HRC-1012

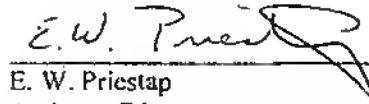
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

agency record for any lawful and authorized purpose, to include responding to FOIA requests.

- b. (U//~~FOUO~~) Except for those Retrieved Materials that are determined by DOS to be DOS agency records, DOS will not, absent written consent of the FBI, disclose or disseminate the Retrieved Materials to anyone other than individuals participating in, assisting, or supervising the DOS record determination process.
  - c. (U//~~FOUO~~) Upon completion of DOS's agency record review, any Retrieved Materials determined not to be DOS agency records, and any copies of such Retrieved Materials made by DOS, will be returned to the FBI for disposition in accordance with FBI policies and procedures.
8. (U//~~FOUO~~) The Parties understand and agree that, until a document within the Retrieved Materials is determined to be a DOS agency record, the Retrieved Materials shall not constitute DOS agency records under the FOIA or any other law; DOS may not integrate the Retrieved Materials into its records filing systems and may not disseminate or use the Retrieved Materials for any purpose other than DOS agency record determination; and if DOS receives a request for access to the Retrieved Materials from outside DOS under the FOIA or any other law or authority, DOS will notify the FBI of the request.
9. (U//~~FOUO~~) The Parties understand and agree that the FBI will mark the Retrieved Materials with appropriate classifications to the greatest extent possible, but that the FBI was unable to obtain definitive classification determinations for all documents therein.

  
\_\_\_\_\_  
Brian J. Egan  
Legal Adviser  
U.S. Department of State

7.19.16  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
E. W. Priestap  
Assistant Director  
Counterintelligence Division  
Federal Bureau of Investigation

07/20/2016  
\_\_\_\_\_  
Date

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

8/5/16  
Serial 182

b6 per  
b7C FBI

HRC-1014

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/2016

b6 per DOS, FBI  
b7C per DOS, FBI

On August 5, 2016, Special Agent [redacted] provided [redacted] of the United States Department of State, Diplomatic Security Service, a package containing the following two (5) DVDs:

Final Production to U.S. Department of State, Disc 2; Dataset 4  
Final Production to U.S. Department of State, Disc 3; Dataset 5-9  
Final Production to U.S. Department of State, Disc 4; Dataset 10-14  
Final Production to U.S. Department of State, Disc 5; Dataset 15-19  
Final Production to U.S. Department of State, Disc 6; Dataset 20

A copy of the FD-597 [Receipt for Property] signed by [redacted] acknowledging the receipt of said DVDs is enclosed in an accompanying 1A.

b6 per  
b7C DOS

Investigation on 08/05/2016 at Washington, D.C.

b3 per FBI  
b7E per FBI

File # [redacted] - 182 Date dictated N/A

By SA [redacted]

b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-1015



Serial 185

HRC-1016



-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/31/2016

b6 per DOS, FBI  
b7C per DOS, FBI

On August 18, 2016, Special Agent [redacted] provided [redacted] of the United States Department of State, Diplomatic Security Service, a package containing one CD-R labeled (U) Final Production to U.S. Department of State, Datasets 1-20 File Listings.

b6 per DOS  
b7C per DOS

A copy of the FD-597 [Receipt for Property] signed by [redacted] acknowledging the receipt of the CD-R is enclosed in an accompanying 1A.

Investigation on 08/18/2016 at Washington, D.C.

b3 per FBI  
b7E per FBI

File # [redacted] Date dictated N/A

By SA [redacted]

b6 per FBI  
b7C per FBI

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-1017

FD-340c (4-11-03)

File Number

[Redacted]

b3  
b7E

Field Office Acquiring Evidence

NF

Serial # of Originating Document

4

Date Received

9/2/2015

From

[Redacted]

b6  
b7C

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MIDYEALE Exam

Reference:

FD-302

(Continuation of Enclosing Material)

Description:

☒ Original notes re interview of

[Redacted]

b6  
b7C

1A3

HRC-100

TOPIC:

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T80 NSICG

FILE UNDER:

currently HB/  
Former DS  
Agent  
till [redacted]

09 - 2 day [redacted] b6 Per FBI, DOS  
b7C Per FBI, DOS

PRE - BEST GIFT LEADERS

[redacted] - Clinton 2007-2009 (HRC)

MAJOR STATE

STARK DIFF in SEC of PERSON

History in line to HRC

- embassies / embassies

ADVERSE SITUATION

- damaged for staff safety

- she overcame safety concerns

- crit. govt. her / short

safety

- at - american government

[redacted]

[redacted] - was prior

- West Bank - b6 Per FBI, DOS

- Asked to open window b7C Per FBI, DOS

- Protocol breaches abundant

- Frequently disobeyed protocols

- insisted window be opened

on occupied territory

Post 1 -

- Removal of lamps & furniture

from Post 1 and took them to

residence

HRC-1093

TOPIC:

DATE:

FILE UNDER:

PAGE:

b7E Per DOS

- Refused to coin up SS labor

Blackburn -

b7E Per DOS

DS Agent of Un. Team

DS Agent Resumed to WATCO BO

DS Agents left him outside

Part of State

b6 Per

b7C DOS

RS: Patrols, brochures, etc.

Having had much more power than  
indicate COS & often overrule  
protocols etc.

CL-in - perception that SAS  
was not simply way to comparison  
for forces. Took select media  
to her room where that should  
her in standard light. often  
breached protocols & steps to  
get good press for  
"Campaign".

HRC-1094

HSI Agents & FSO

# 4

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

5

Date Received

9/11/15

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

U.S. DEPT OF STATE

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (c)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MID YEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

b6  
b7C

DEPARTMENT OF STATE (S/ES-IRM)

HRC-1095

SES = Office of the Secretary, Office of  
the Executive Secretary

9/11/2015

@ESOC in Culpeper, VA  
Backup @ HST

b6  
b7C

Unclass (open net)

Class (classnet)

DS,  
consular affairs,  
etc.

SES (one domain  
of many)

DS,  
consular affairs,  
etc.

SES (one domain  
of many)

Information Resource Management  
S/ES-IRM

POEMS - originally a TS network for email  
- only INR has TS network

state keeps copies for an indefinite  
period of time

~600 customers, take snapshots of customers' files  
and emails as they come and go

Have backup tapes (system wide  
backup of exchange, file server,  
shared drive) of class and unclass.

b6  
b7C

Some addresses were distr. lists - lists different currently  
than they were in 2011. Baglioni works here probably

IRM-POC-Ax

Backups only held for 45 days

typically keep mailbox for  
60 days, then  
deleted

- SES also responsible for assigning devices - keep property records only until returned.
- System used to issue devices at the time was taken offline; efforts to get back in unsuccessful - data corrupt
- Customers do not use SMART for archiving - other parts of state
- Guidance for backup is "print and file"
- PACE - people/staff close to Secretary may be on this system (small number)  
↳ belongs to bureau of diplomacy

HRC-1096

2-10)

Express (replaced by SMART)

- ↳ created to make archive of telegraphs
- ↳ phased out ~4-5 years ago

Openet + Openet+ (plus) are same

- ↳ added web browsing and external email

No official restriction <sup>+2011</sup> on using personal email

- guidance in 2009 to send work-related email sent to personal email back to work account
- one → openet everywhere → Go (global openet)
- Global openet (uses FOB to access from any computer)

→ users on travel who don't have mobile device might do this.

- No mechanism to track use of personal email
- Customers not requested to <sup>provide</sup> ~~use~~ personal email address
- No record of form completed requesting ~~an~~ unclass or class account for Secretary Clinton
- Very strict on form requirement
- No request for mobile device

b6  
b7C

**Purpose:** Need to understand IT / Email ecosystem to provide further guidance wrt preservation requests sent to DoS.

**Questions:** What are the primary email systems for each classification level (Uncl, S, TS):

- What type of information is conveyed on these systems (i.e., general coms, cables, exec communications, etc)?
- How are users allocated between systems and how can we identify if a specific person has a profile on a given system?
- How is the data stored for each system?
  - What is the frequency of backup (i.e. automatic, user initiated), how far back does it go?
  - Where is this information stored (i.e., remote server vs. desktop PST)
- What is the retention system for each system?
- Do these systems use the State Messaging and Archival Retrieval Tool (SMART)?
  - How can SMART records be accessed?
- What are the search and filtering capabilities for archived files on each system?
- Who is a POC for each system?
- Is there a POEMS equiv for unclass or TS coms?
- Does POEMS communicate with Siprnet systems, unclass systems, etc?
- What system would the Secretary of State be on?

Classification	Uncl	Secret	TS
Domain	Opennet Opennet+ → <i>add USS</i>	Classnet	JWICS
Email Domain	State.gov	State.sgov.gov	
Sub Systems	<ul style="list-style-type: none"> <li>DoS Outlook email</li> <li>Personal email</li> <li>PACE (Public Affairs Communications Electronically)</li> </ul>	<ul style="list-style-type: none"> <li>POEMS (Principal Officer Electronic Messaging System)</li> <li>CableXpress</li> <li>not claimant</li> <li>just telegram</li> </ul>	
Technical Point of contact		POEMS	
Primary Users	All DoS employees PACE - Public Affairs Media	POEMS - 7 <sup>th</sup> Floor Execs	

b6  
b7C

b6  
b7C



1A5

FD-340 (Rev. 4-11-03)

File Number [REDACTED] - 302

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 6

Date Received 9/17/15

From [REDACTED]  
(Name of Contributor/Interviewee)

b6  
b7C

DOPT OF STATE  
(Address)

(City and State)

By [REDACTED]

b6  
b7C

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: MID YEAR EXAM

Reference: \_\_\_\_\_  
(Communication Enclosing Material)

Description: ☒ Original notes re interview of

[REDACTED]

b6  
b7C

1A5

DOS

9/17/15

120 MB total 700K (400 central)

100 & spoke over 100 of existing

central location, each spoke embassy or consulate

SES remaining?

Managed by own <sup>appropriate</sup> ISSO's Group

IRM

contact Info Sec. Officer

Backup for server

OS

VM is backed up with Snap

Just another month or so)

DB is on separate luns (don't get backed up) re: authority

Exported incl. deleted items -> preserved

Have DAGS copies of every DB One Active DB (transactions are written

" Dumpster for 90 days

to other copies of DB)

Retention

Posts do have backups kept varying lengths based on storage limitations

↳ Varies by post

↳ off-site backups, but may vary by location (practice may vary)

Profiles centrally located open net & ? (approx 400 profiles)

IRM

b6

b7C

Mailboxes - short turnaround (1 day) 500MB mail

↳ challenge is the date timeframe

5G mail - most of 2012

by 2013

Record email - Nat. Arch

includes the RI for 90 days

reflects official direction

Smart Archive AGIS - Peggy Graphil Deputy Asst. Sec. Email Cables & records -> Records Management Bureau

↳ in 2008,

fully operation 2010

↳ official communication

SES chosen not to go Smart Archive - obligation to Print/File

↳ Senior officials - retention policy archived when departing

Prior was

Cable Express

9/17/15

b6  
b7C

[Redacted]  
[Redacted]

- STATUS OF PRESERVATION REQUEST
- BACKUP CAPABILITIES (PROCESS, RETENTION PERIOD)
- USER SPECIFIC RECORDS
- TURN AROUND TIME
- INR CONTACT [Redacted] → [Redacted] POC [Redacted]

b6  
b7C

120K MAIL BOXES

95  
35K CENTER LINE NBS

KIB/SPOKE  
↓  
CREATES

IRM (HUBS) → DAGS  
PST/ISSD (SPOKES) → DATA CENTER

400 of 900 in center

majority in ISSD

PST → ENTERED

ENTER ENTERED  
PST → RECORD EMAIL

100 of Billion  
EMAILS TO  
FIREWALL  
80% STOPPED  
HERE

exported all MAILBOXES FOR USERS ON LIST (for people in center)

deleted items retained FOR 90s, stored on 5 disks 2 side

- DO NOT INCLUDE desktop ARCHIVED FILES

MAILBOX CAP

ONLY WHAT IS IN THE ACTIVE MAILBOX

SCANS → NOT LIKELY A LOT OF OLD EMAILS DUE TO LIMITS

300 GB  
in 2012/2013 → DELETE OR PST

→ RECORD EMAIL SYSTEM

SMART - 2008  
AGIS 2010  
2010  
AGIS 2010  
2010

DATE LETTER HOLD

SNAP SHOT OF MAILBOX

NO RECORDS FOR THOSE TH. LIST

SE OFF, 100 A BUREAU OFFICIAL RECORDS

- course of action of policy  
- underpinning of policy  
- Add

varying retention  
period  
by topic

#8

1A8

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3

b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

9

Date Received

9/24/15

From

~~WFO~~

[Redacted]

WILMERHALE

(Name of Contributor/Interviewee)

b6

b7C

1875 PENNSYLVANIA AVE NW

(Address)

WASHINGTON, DC 20006

(City and State)

By

[Redacted]

b6

b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☒ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

~~PROPERTY RECEIPT~~

~~LETTER FROM WILMERHALE~~

1A8

HRC-1107

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T80 NSICG

Case ID: \_\_\_\_\_

On (date) SEPT 24, 2015

item (s) listed below were:

- ☐ Collected/Seized  
☒ Received From  
☐ Returned To  
☐ Released To

(Name) WILMER HALE(Street Address) 1875 PENNSYLVANIA AVE NW(City) WASHINGTON DC 20006

Description of Item (s): \_\_\_\_\_

(1) LAPTOP - APPLE MAC BOOK AIRS/N

b6

b7C

b6

b7C

9/24/2015

HRC-1108

b6

b7C

Received By: \_\_\_\_\_

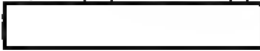
Received From: \_\_\_\_\_

Printed Name/Title: \_\_\_\_\_

Printed Name/Title: \_\_\_\_\_

Delivered 09242015

1. One (1) silver Apple brand Mac Book Air laptop computer, Serial Number



b6  
b7c

*Copy*

WILMERHALE

September 10, 2015

[REDACTED]  
National Security Division  
Department of Justice  
Washington, D.C. 201530

By Email: [REDACTED]

Dear [REDACTED]

b6  
b7C

b6  
b7C

Thank you for talking with us on September 8 and 9, 2015, regarding our voluntarily providing the FBI two laptop computers and one external hard drive that belong to Justin Cooper. We have described these devices (hereinafter "Mr. Cooper's computer hardware") more fully in the enclosed document. This letter memorializes our agreement with the government about the removal of Mr. Cooper's personal and business files from Mr. Cooper's computer hardware.

As we discussed and as the government has agreed, before providing Mr. Cooper's computer hardware to the FBI, we will remove and securely delete Mr. Cooper's personal and business files. We will load personal and business files selected by Mr. Cooper onto a new computer owned by Mr. Cooper, and he will be free to retain and use that data in the ordinary course without restriction. WilmerHale will maintain and securely store a complete copy of all personal and business files removed from Mr. Cooper's computer hardware until such time that we reach a written agreement with the government as to what portion we should retain.

The following files will remain on Mr. Cooper's computer hardware when it is provided to the FBI: (1) Mr. Cooper's emails to and from Secretary Clinton while she was in office extracted from his email files; and (2) back-up copies of Secretary Clinton's blackberry device. As we discussed and agreed regarding our consent for these remaining files on Mr. Cooper's computer hardware:

1. We authorize the government to possess and review all of Mr. Cooper's emails to or from Secretary Clinton while she was Secretary of State (January 21, 2009, to February 1, 2013). During that time, Secretary Clinton occasionally sent Mr. Cooper emails for hand-delivery to her husband, President Clinton. We are aware that some of those emails contain information marked "Attorney Client Privilege."
2. We authorize the government to possess files labeled as back-up copies of Secretary Clinton's blackberry device. These files do not belong to Mr. Cooper and we therefore lack the authority to consent to an examination of their contents.

Mr. Cooper's computer hardware contains one or more files labeled as back-up copies of blackberry devices, but that are not further labeled with an owner's name.

WILMERHALE

September 15, 2015  
Page 2

b6  
b7C

As we discussed and as the government has agreed, we will open those files<sup>\*</sup> for the sole purpose of determining whether one or more of them is a back-up copy of Secretary Clinton's blackberry device. Any file determined to be a back-up copy of her blackberry device will remain on Mr. Cooper's computer hardware and be provided to the FBI. As with the files labeled with Secretary Clinton's name, these files do not belong to Mr. Cooper and we therefore lack the authority to consent to an examination of their contents.

Mr. Cooper will not transfer, copy, or retain in any form the files that will remain on Mr. Cooper's computer hardware provided to the FBI.

Sincerely yours,

b6  
b7C

---

<sup>\*</sup> Our forensics team will first copy these files to an external drive and open and review them in that location. Our team will not open those files on the original machine.

HRC-1111



Justin Cooper's Computer Hardware

- A. One (1) silver Apple brand Mac Book Air laptop computer, Serial Number C02LF01CFM74
- B. One (1) silver Apple brand Mac Book Pro laptop computer, Serial Number W89361H6644, and charging cord
- C. One (1) black Seagate brand external hard drive, Serial Number NA5AGV8A, and USB cord

*Cerf*  
WILMERHALE

September 24, 2015

[REDACTED]  
National Security Division  
Department of Justice  
Washington, D.C. 201530

By Email: [REDACTED]

Dear [REDACTED]

b6  
b7C

b6  
b7C

Pursuant to our letter agreement with the government dated September 10, 2015, today we voluntarily provided the FBI one silver Apple brand Mac Book Air laptop computer, Serial Number C02LF01CFM74 ("Mac Book Air"), that belongs to Justin Cooper.<sup>1</sup> We provided the Mac Book Air for the purposes of DOJ/FBI's investigation of Secretary Clinton's personal email accounts.


As agreed, we have securely deleted from the Mac Book Air Mr. Cooper's personal and business files, and we have overwritten its unallocated space with zeros. WilmerHale is maintaining and securely storing a complete copy of all personal and business files removed from the Mac Book Air until such time that we reach a written agreement with the government as to what portion we should retain.

The following files remain on the Mac Book Air: (1) Mr. Cooper's emails to and from Secretary Clinton while she was in office extracted from his email client and (2) back-up copies of Secretary Clinton's blackberry device. The attached document describes in greater detail the files remaining on the Mac Book Air. As we agreed on September 10, 2015, regarding our consent for the files remaining on the Mac Book Air:

1. We authorize the government to possess and review all of Mr. Cooper's emails to or from Secretary Clinton while she was Secretary of State (January 21, 2009, to February 1, 2013). During that time, Secretary Clinton occasionally sent Mr. Cooper emails for hand-delivery to her husband, President Clinton. We are aware that some of those emails contain information marked "Attorney Client Privilege."
2. We authorize the government to possess the files labeled as back-up copies of Secretary Clinton's blackberry device. These files do not belong to Mr. Cooper and we therefore lack the authority to consent to an examination of their contents.

<sup>1</sup> We will provide the FBI an additional laptop computer and an external hard drive that also belong to Mr. Cooper at a later date.

<sup>2</sup> We treated any email addressed to or from Mr. Cooper as his email. As such, the Mac Book Air contains not only those emails that were sent between Mr. Cooper and Secretary Clinton, it also contains emails that were addressed to both Mr. Cooper and Secretary Clinton (within the same email).

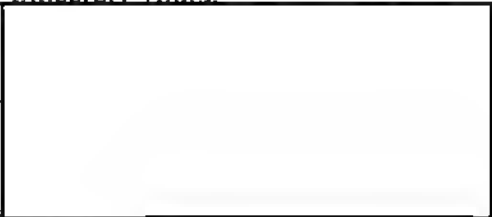
  
September 24, 2015

Page 2

The Mac Book Air contained one or more files labeled as back-up copies of blackberry devices, but that were not further labeled with an owner's name. As we discussed and as the government agreed, we opened those files<sup>3</sup> for the sole purpose of determining whether one or more of them was a back-up copy of Secretary Clinton's blackberry device. None of those files contained an email account belonging to Secretary Clinton.

Mr. Cooper has not transferred, copied, or retained in any form the files that remain on the Mac Book Air. WilmerHale is temporarily holding an image of the Mac Book Air hard drive (which includes the files that remain on the Mac Book Air); we created this drive to enable us to restore data in the event our forensics team made an error when segregating and removing data. We are not aware of our forensics team making any errors, thus we will securely delete the image of the Mac Book Air in seven calendar days from today unless you advise us in writing that the files listed on the attachment (*i.e.*, the files remaining on the Mac Book Air) are corrupted or that their contents are otherwise irretrievable for reasons that could be cured with the image of the Mac Book Air. After we provide Mr. Cooper's remaining laptop to the FBI, and after a similar waiting period, we will degauss the drive that contains the image of the Mac Book Air drive.

Sincerely yours,

b6  
b7c  
Enclosure

<sup>3</sup> Our forensics team first copied these files to an external drive and opened and reviewed them in that location. Our team did not open these files on the Mac Book Air.



Enclosure // 09/24/2015

All items reside in \Users\Jcooper\Desktop (Item numbers have no significance; item numbers used here for reference only)

Item 1

drwxr-xr-x@ 5 502 20 170 Sep 15 18:15 Archive\_email.mbox

Item 2

dr-xr-xr-x 1161 502 20 39474 Sep 16 12:45 Archive\_email\_documents

Item 3

-rw-r--r-- 1 502 20 66559 Sep 21 11:45 Archive\_responsive\_2009  
Jan and Feb.rtf

Item 4

-rw-r--r-- 1 502 20 5641 Sep 21 12:05 Archive\_responsive\_2009  
March.rtf

Item 5

-rw-r--r--@ 1 502 20 17040306 Feb 26 2013 HR BlackBerry Bold  
9900.ipd

Item 6

-rwxrwxrwx 1 502 20 25446688 Apr 13 2009 hrc  
Backup-(2009-04-13).ipd

Item 7

-rw-r--r-- 1 502 20 26283514 Nov 26 2011 hrc BlackBerry Curve  
(24B603D0) (2011-11-26) - Full.bbb

Item 8

drwx----- 5 502 20 170 Aug 15 12:39 hrc saved

Item 9

-rw-r--r-- 1 502 20 385147 Nov 26 2011 hrc saved.bbb

Item 10

-rw-r--r-- 1 502 20 385147 Nov 26 2011 hrc saved.xml

Item 11

-rw-r--r-- 1 502 20 385147 Nov 26 2011 hrc saved.zip

HRC-1115

#12

1A12

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

14

Date Received

10/5/15

From

WILMER HALE

(Name of Contributor/Interviewee)

1975 PENNSYLVANIA AVE NW

(Address)

WASHINGTON DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☒ Yes

☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

LETTER FROM WILMERHALE AND

PROPERTY RECEIPT

1A12

HRC-1124

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T80 NSICG

Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property

Case ID: \_\_\_\_\_

On (date) OCT 5, 2015

item (s) listed below were:

- ☐ Collected/Seized  
☒ Received From  
☐ Returned To  
☐ Released To

(Name) WILLERHALE(Street Address) 1875 PENNSYLVANIA AVE NW(City) WASHINGTON DC 20006Description of Item (s): MAC BOOK PROS/APOWER CORDb6  
b7Cb6  
b7C10/5/2015  
837

Received By

(Signature)

Received From:

Printed Name/Title

Printed Name/Title:

b6  
b7C

FBI Copy

WILMERHALE

October 5, 2015

[REDACTED]  
National Security Division  
Department of Justice  
Washington, D.C. 201530

b6  
b7C

By Email: [REDACTED]

b6  
b7C

Dear [REDACTED]

Pursuant to our letter agreement with the government dated September 10, 2015, today we voluntarily provided the FBI one silver Apple and MacBook Pro laptop computer, Serial Number W893611H6644 ("MacBook Pro"), that belongs to Justin Cooper.<sup>1</sup> We provided the MacBook Pro for the purposes of DOJ/FBI's investigation of Secretary Clinton's personal email accounts.

As agreed, we have securely deleted Mr. Cooper's personal and business files from the MacBook Pro, and we have overwritten its unallocated space with zeros. WilmerHale is maintaining and securely storing a complete copy of all personal and business files removed from the MacBook Pro until such time that we reach a written agreement with the government as to what portion we should retain.

The following files remain on the MacBook Pro: (1) Mr. Cooper's emails<sup>2</sup> to and from Secretary Clinton during her tenure as Secretary of State extracted from his email files; and (2) back-up copies of Secretary Clinton's blackberry device. The attached document describes in greater detail the files remaining on the MacBook Pro. We resolved several issues for the MacBook Pro as follows:

- Using MD5 hash values, Kroll determined that two text files on the MacBook Pro were identical to two text files on the MacBook Air provided to the FBI on September 24, 2015. As we agreed, because those files are identical and had therefore already been preserved in Kroll's processing of the MacBook Air, we did not review and save the responsive portions of those two files on the MacBook Pro.
- Again using MD5 hash values, Kroll determined that two text files on the MacBook Pro were identical to each other. As we agreed, because those files were identical to each other, Kroll processed only one of them.

<sup>1</sup> We will provide the FBI an external hard drive that also belongs to Mr. Cooper at a later date.

<sup>2</sup> We treated any email addressed to or from Mr. Cooper as his email. As such, the MacBook Pro contains not only those emails that were sent between Mr. Cooper and Secretary Clinton, it also contains emails that were addressed to both Mr. Cooper and Secretary Clinton (within the same email).

October 5, 2015

Page 2

- Like the MacBook Air, the MacBook Pro contained files labeled as back-up copies of blackberry devices, but that were not further labeled with an owner's name. Kroll matched those files to [REDACTED] labeled blackberry back-up files on Mr. Cooper's MacBook Air using MD5 hash values. As described in my letter of September 24, 2015, Kroll had previously determined those files on the MacBook Air did not contain an email account belonging to Secretary Clinton.

As we agreed on September 10, 2015, regarding our consent for the files remaining on the MacBook Pro:

- We authorize the government to possess and review all of Mr. Cooper's emails to or from Secretary Clinton while she was Secretary of State (January 21, 2009, to February 1, 2013). During that time, Secretary Clinton occasionally sent Mr. Cooper emails for hand-delivery to her husband, President Clinton. We are aware that some of those emails contain information marked "Attorney-Client Privilege."<sup>3</sup>
- We authorize the government to possess the files labeled as back-up copies of Secretary Clinton's blackberry device. These files do not belong to Mr. Cooper and we therefore lack the authority to consent to an examination of their contents.

Mr. Cooper has not transferred, copied, or retained in any form the files that remain on the MacBook Pro. WilmerHale is temporarily holding an image of the MacBook Pro hard drive (which includes the files that remain on the MacBook Pro and the text files described above) to enable us to restore data in the event our forensics team made an error when segregating and removing data. We are not aware of our forensics team making any such errors, thus we will securely delete the image of the MacBook Pro and degauss the drive in seven calendar days from today unless the government advises us in writing that the files listed on the attachment (i.e., the files remaining on the MacBook Pro) are corrupted or that their contents are otherwise irretrievable for reasons that could be cured with the image of the MacBook Pro hard drive.

Enclosure

b6  
b7c

Enclosure

<sup>3</sup> Because Mr. Cooper's emails contain information marked "Attorney-Client Privilege," David Kendall, counsel to Secretary Clinton, is reviewing Mr. Cooper's emails.



**ATTACHMENT**

**JG Cooper MacBook Pro // 10022015**

(Item numbers have no significance; used here for sake of reference)

**Item 1**

hrc saved 2

macbook pro\Single Files\pro - responsive\hrc saved 2

**Item 2**

hrc BlackBerry Curve (24B603D0) (2011-11-26) - Full.bbb

bbb 10/2/2015 0:00 10/2/2015 16:49 1c3c62e765f7b85d9cc35f3c0cf57f7c  
macbook pro\Single Files\pro - responsive\hrc BlackBerry Curve (24B603D0) (2011-11-26) - Full.bbb

**Item 3**

hrc saved.bbb

bbb 10/2/2015 0:00 10/2/2015 16:49 bca9c5661494c15c1aaf8902cc9ab11  
macbook pro\Single Files\pro - responsive\hrc saved.bbb

**Item 4**

HR BlackBerry Bold 9900.ipd

ipd 10/2/2015 0:00 10/2/2015 16:49 acaf592275644075510cf53110df4567  
macbook pro\Single Files\pro - responsive\Mail Download\HR BlackBerry Bold  
9900.ipd

**Item 5**

hrc saved (folder)

**Item 6**

hrc Backup-(2009-04-13).ipd

ipd 10/2/2015 0:00 10/2/2015 16:49 af8ad110a4faf0fa4234fa6151675f6f  
macbook pro\Single Files\pro - responsive\hrc Backup-(2009-04-13).ipd

**Item 7**

Archive\_email.mbox

mbox macbook pro\Single Files\pro - responsive\Archive\_email.mbox

**Item 8**

Responsive - PC Mail - Sent Items.mbox

mbox macbook pro\Single Files\pro - responsive\Responsive - PC Mail - Sent Items.mbox

**Item 9**

responsive PC Mail inbox old server inbox.rtf

rtf 10/2/2015 0:00 10/2/2015 16:49 18ed6542b5c4ab3f69384bdbbc7d3fa2  
macbook pro\Single Files\pro - responsive\responsive PC Mail inbox old server inbox.rtf

**Item 10**

responsive PC Mail Inbox.rtf

rtf 10/2/2015 0:00 10/2/2015 16:49 ac71599abc6d62ff95482cc7c8012f9a  
macbook pro\Single Files\pro - responsive\responsive PC Mail Inbox.rtf

**Item 11**

hrc saved.zip

zip 10/2/2015 0:00 10/2/2015 16:49 bca9c5661494e15c1aa1f8902ce9ab11  
macbook pro\Single Files\pro - responsive\hrc saved.zip

**Item 12**

hrc saved.xml

xml 10/2/2015 0:00 10/2/2015 16:49 bca9c5661494e15c1aa1f8902ce9ab11  
macbook pro\Single Files\pro - responsive\hrc saved.xml

**Item 13**

Mail Download

macbook pro\Single Files\pro - responsive\Mail Download

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

24

Date Received

10-23-15

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

FBI HQ

(Address)

Washington DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

Midyear Exam

Reference:

Interview Notes

(Communication Enclosing Material)

Description:



Original notes re interview of

[Redacted]

b6  
b7C

1 A

HRC-1155

~~SECRET~~

DOB [redacted]

on w/ Rice

- 6 yrs DS

was on detail @ same  
time, but now w/ IRS.

b6 per  
b7C FBI

LAFO -

Detail - [redacted] w/ Rice -

b6 per  
b7C FBI  
b7E Per DOS

[redacted]

Chap address - would usually take [redacted] hut.  
from DCA to White Plains - take her back & forth  
USSS handled most security [redacted]

b6 per  
b7C FBI  
b7E Per DOS

DSS - SAC (SES) [redacted]  
ASAC - [redacted] (over shift Admin)  
SSA for shifts  
SAs between shifts

all still  
w/ DSS.

[redacted] - direct SSA over RM  
[redacted] - WFO/DSS - both SAs on details  
[redacted] - WFO/DSS

b6 per  
b7C FBI

~~SECRET~~

@ DOS. 7th Floor

b7E Per DOS

① / drop phones on DSS office on 2nd floor  
b. [redacted] orcade.

Blackberry -  
don't recall computer in office

Sec Clinton would keep phone in  
out to get phone & go to  
Call.

top  
Drawer

& come  
space to make

b7E Per DOS

Huma  
Cheryl - offices inside [redacted]

didn't travel  
much overseas

constantly on device - can't remember

b6 per  
b7C FBI  
b7E Per DOS

Main  
traveling  
crew

Jake Sullivan

(Mostly on trips)

can't recall specifics of devices used by above  
but prob blackberries

POSS  
gmail

b7E Per DOS

Never interacted w/ Sec or Cheryl via email but  
sometimes forwarded.

Clintonfoundation.org

Know I res<sup>in DE</sup> had secure phone - would assume  
secure room, but not sure.

~~SECRET~~

Security Engineers / Specifically assigned to SecState.  
DSS team Tech ~~Spent~~ traveled overseas to set up COMMS.  
(usually @ hotel)

Welcome letter provided by RSD to DSS concerning guidance on Security in Country. Not sure what was provided to Sec & direct staff

Horwath after w/ Advance vs. Supervisors but RSD not part of it.

between RSD cables prop go back to SAC re security issues. DSS <sup>DSS</sup> SSA <sup>RSD</sup> in charge of 7th floor.

DSS for  
DIP POUCH - COMMS

but as far as Sec. mostly processed

b7E Per DOS

b6 per  
b7C FBI

Scheduler - would have contact to determine location, departure time

During Sweeps OCONUS.

b1 Per DOS  
b7E Per DOS

HRC-1158

~~SECRET~~

1A23

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

27

Date Received

11/6/2015

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

U.S. Department of State

(Address)

(City and State)

By

ITS/FE

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MIDYER EXAM;  
MISHANDLING OF CLASSIFIED  
UNKNOWN SUBJECT OR CONCEPT  
SENSITIVE INVESTIGATION (TOP SECRET/FOUO)

Reference:

(Communication Enclosed/Reference)

Description:

☒ Original notes to interview of [Redacted]

Copy of email from Senior Special Agent

[Redacted]

U.S. Department of

State, dated 11/6/2015.

b6  
b7C

HRC-1159

[REDACTED] (WF) (FBI)

**From:** [REDACTED] (OIG) [REDACTED]  
**Sent:** Friday, November 06, 2015 12:01 PM  
**To:** [REDACTED] (WF) (FBI)  
**Subject:** Case email

b6 per DOS, FBI  
b7C per DOS, FBI

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Look for

FW: 2003 Cable

Or

[REDACTED]  
[REDACTED]  
Senior Special Agent  
Office of Investigations  
Office of the Inspector General  
US Department of State  
[REDACTED] office  
[REDACTED] cell

b6 per DOS, FBI  
b7C per DOS, FBI



1A24  
FD-340 (Rev. 4-11-03)

File Number

-302

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

28

Date Recd

12/29/2015

From

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

By

SA

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)  
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

b6  
b7C

Title:

MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED

Reference:

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

FD-597 + State Department  
Property Transaction

HRC-1161



U.S. Department of State

[illegible]

HRC-1162

**GENERAL INSTRUCTIONS**

- (1.) **Date**  
Enter the date the form DS-584 is prepared.
- (2.) **Action**  
Enter an "X" in the select action field to indicate the type of property action.
  - Issue - asset(s) issued to or moved from the warehouse or storage facility to an employee, office, residence, or other location.
  - Turn In - asset(s) turned in or moved from an employee, office, residence, or other location back to the warehouse or storage facility.
  - Loan - asset(s) provided to an entity (see 14 FAM 411.2) for a period of less than 90 days and/or no more than a year.
  - Reutilization - the movement of an asset from one location to another. The movement of an asset from one bureau or post to another bureau or post.
  - Transfer - the movement of asset(s) from one location to another where title is passed.
- (3.) **Control/Authorization Number**  
System generated by ILMS.
- (4.) **Loan Information**  
Enter the date the loan ends and the date the loan is due.
- (5.) **Requestor's Name (Print Name)**  
Enter the name of the receiving agency/post/bureau contact.
- (6.) **Post/Agency/Bureau**  
Enter the name of the receiving agency/post/bureau.
- (7.) **Office**  
Enter the name of the office.
- (8.) **Room Number**  
Enter the room number.
- (9.) **Telephone Number**  
Enter the telephone number of the receiving agency/post/bureau contact.
- (10.) **Justification or Remarks**  
Enter the reason for the request and any other item specific details.
- (11.) **Authorizing Officer (Print Name)**  
Enter the authorizing officer name.
- (12.) **Authorizing Officer (Signature) and Date (mm-dd-yyyy)**  
Enter the authorizing officer signature and date (14 FAM 411.2, 14 FAM 414, and 14 FAM 425).
- (13.) **Approving Officer (Print Name)**  
Enter the approving officer name.
- (14.) **Approving Officer (Signature) and Date (mm-dd-yyyy)**  
Enter the approving officer signature and date (14 FAM 411.2, 14 FAM 414, and 14 FAM 425).
- (15.) **Deliver or Ship to (List Registry Information)**  
The delivery address of the agency to which the property is being transferred.
- (16.) **Property Details**
  - Property Number -**  
Enter the nonexpendable property application (tag) property number.
  - Serial Number -**  
Enter any serial number.
  - Description -**  
Enter description.
  - Quantity -**  
Each line will be a one-item entry.
  - Condition -**  
Indicate the condition of the property.
  - Unit Cost -**  
Enter the unit cost.
  - Total Cost -**  
Enter the total cost.
- (17.) **Property Records**  
Update property records.
- (18.) **Receipt**  
The receiving agency's employee signs and dates (14 FAM 413.3).

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # \_\_\_\_\_

On (date) 10/29/2015

item(s) listed below were:  
☒ Received From  
☐ Returned To  
☐ Released To  
☐ Seized

(Name)

(Street Address) 2025 E St., NW

(City) Washington, DC

Description of Item dc 5850 desktop computer 4N

b6  
b7C

HRC-1164

Received By:

Received From:

(Signature)

b6  
b7C

#26

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302-1A

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

30

Date Received

11/3/2015

From

[Redacted]

(Interviewee)

b6  
b7C

805 21<sup>ST</sup> NW Suite 400

(Address)

WASHINGTON DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Title:

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

[Redacted]

on 11/3/15

b6  
b7C

HRC-1167

11-3-15

b6  
b7C

Didn't speak to DOS about same matter

1st of emails released / contacted by Vice Media  
title "WikiLeaks" - redacted.

@ DOS Feb 09 - end of Sec term

[redacted] met w/ HC. Volunteered to take  
Dep Sec off to [redacted]

b6  
b7C

[redacted] under Pres. Clinton

"Clintonista"

99 - @ Pentagon [redacted] rpt.

2003 - Hire #13

2009 - conversation about [redacted]

b6  
b7C

requested DOS

[redacted] - initial spokesperson

[redacted] - TS//SI clearance

Confirmed <sup>Thurs 64</sup> Memorial Day

[redacted] took over  
in both roles.

Sworn in day after M. day 2009

Met w/ Sec @ 8:45 every morning

in many bilateral mtgs.


Saw Sec. 4-5 times a day - most interactions  
in person.

didn't email a lot.

2010 (April) got sense of WikiLeaks

2010 (Nov) came about fully

would try to guide as to why certain info shouldn't be put out.

General Rule  wouldn't talk about classified material contained in a cable but would find ways to talk about stuff w/o talking about the classified

Most of Dec / Born daily & no mtgs in Malls office to manage Wikileaks.

w/ Wiki "playing defense" most of time.  
batting av. 250 / 300 gave it best shot

would highlight not to post in entirety or would provide background so wouldn't misread cables.

outside of Wikileaks —

how to talk about diplomatic conversation in public sphere  
w/o getting into details that may be confidential / protected.

Respect what has come out of Benghazi  
ex. look back & determine something was classified even though thought was it wasn't @ time

HC Inner Circle

Cheryl Mills - lead / COS

Huma  
Jace } always w/ Sec.

usually would go through Mills, but sometimes would go direct w/ HC.

judgement call on what provided by email.  
no guidance

"Didn't think it was a big deal she didn't use DOS email."

HC very much a paper person.  
"paper drove system" email

decisions always made re: "How do I deliver this fact w/o compromising sources & methods?"

Mtg. w/ NY Times Ed. Nov 2010 @ DOS

re: classified info now in open space.

Told - not to access NYT from work, but okay @ home.

Did not have any Jan - daily conversations w/ [redacted]

b6  
b7c

Would cite cable #s and asked for comments before release.

Attempted to set rules -

NYT would pass off to other outlets.

NYT would remove some names



Nobody comes to mind as a blatant security violator.

(TPs)

generally ~~positioned~~ on low side  
comm. ~~level~~ <sup>closer</sup> to original  
she ~~is~~ <sup>is</sup> other equities who may have

Desk officers know "protect sources/methods"

No <sup>security</sup> concerns looking back @ how HC handled  
her comms during her time @ DOS.

Standard comms between PA & Sec through Ops

10 met w/ HC everyday @ 9:45

colleagues outside this group prob emailed  
w/ HC more.

A-bureau  
Pat Kennedy\* - 2<sup>likely</sup> involved w/ setup of email &  
& Mills system used  
by HC

FD-340 (Rev. 4-11-03)

**File Number**

- 302

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 51

Date Received 11-15-15

**From**

(Name of Contributor/Interviewee)

US Dept. of State

(Address)

NW Washington D.C.  
(City and State)

(City and State)

**By**

b6  
b7C

To Be Returned ☐ Yes

☒ No

**Given** : ☐ Yes

☒ No

~~Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)~~  
~~Federal Rules of Criminal Procedure~~

☐ Yes☒ No**Federal Taxpayer Information (FTI)**☐ Yes☒ No

Midyear Exam.

Reference: Interview Notes

(Communication Enclosing Material)

**Description:**

18

Original notes re interview of

b6  
b7C

1A27

HRC-1.172

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T8D NSICG

RELEASE IN  
FULL

**From:** Abedin, Huma <AbedinH@state.gov>  
**Sent:** Sunday, April 10, 2011 10:14 AM  
**To:** H  
**Subject:** Fw: Stevens Update (Important)  
**Importance:** High

Jake may have sent but in case not..

— Original Message —

**From:** Davis, Timmy T  
**Sent:** Sunday, April 10, 2011 06:48 AM  
**To:** Sullivan, Jacob J; Abedin, Huma; Wells, Alice G; S\_SpecialAssistants  
**Subject:** Stevens Update (Important)

*New York  
replaced  
McManus*

(SBU) Per Special Envoy Stevens:

- The situation in Ajdabiyah has worsened to the point where Stevens is considering departure from Benghazi. The envoy's delegation is currently doing a phased checkout (paying the hotel bills, moving some comms to the boat, etc). He will monitor the situation to see if it deteriorates further, but no decision has been made on departure. He will wait 2-3 more hours, then revisit the decision on departure.

- He received reports of shelling last night in Ajdabiyah as well as snipers shooting people in the city. AFRICOM reported Qadhafi's forces took the eastern and western gates of Ajdabiyah, with 5 vehicles at the eastern gate and 50 at the western gate. More Qadhafi forces are heading to Ajdabiyah from Brega.

- The Brits report Qadhafi forces are moving from Sirte to Brega, which they interpret as preparation for another assault on Ajdabiyah today.

- He plans to discuss the situation further with the Brits, Turks, and the TNC to see if this is an irreversible situation. Departure would send a significant political signal, and would be interpreted as the U.S. losing confidence in the TNC. Initial message to the TNC would frame the departure as due to security grounds and as a temporary measure only.

- Polaschik said she would discuss these developments with Amb. Cretz.

- If the group departs, the contract for the boat stipulates they return to Greece. One scenario could be the group stages elsewhere for a few days.

Ops will continue to monitor the situation.

b6  
b7C

Feb 2009 - 2013

↳ Ops Center

Later

Advance Staff -  
"The Line"

March/April 2010 became Clintons

(2)

on travel Special Asst  
12-15 people  
travel w/.

filled in during ho

Info/Action memos - decide what Sec needs to  
Intel Notes see.

INR brings to

PDB Briefing is separate.

(1) 6 AM - 3 PM

(2) 12 - when work is done.

talk of briefing to learn what to brief  
Make sure useful

Reports mix bag:  
some as mundane as  
BCL - brief checklist  
Talking Points not class  
BCL +

ceremony in  
place when Clinton arrived

b6  
b7C

Secret to Codeword - would be careful to make  
sure proper classification put in proper folder  
in office 100% paper - folders clearly marked.

on travel - Communicate w/ line and  
Sec's Xes - Joe McMannus.  
communicate both high & low

Guidance on when to send up?

sort of get a sense of when sent where  
very skittish about sending stuff to anyone  
would originally check w/ XO, but eventually  
got comfortable.

cos

High side / Low side

Jake worked till 11pm - Dept cas Policy

Huma. Dep cas Ops. / concerned about trip logistics

Would have been weird to send HC emails direct.  
possible only direct email during Royal Wedding

Had no knowledge HC working off personal server  
knew ~~didn't~~ had computer on her desk.

\* no electronics in office

~~didn't~~

only showed up as H. odd b/c convention  
usually last, first.

assumed it was DOS b/c knew she had a  
Blackberry.

all office emails came out from time to time

---

2005 w/ Blackwater in Iraq as FSD w/ DOS.  
Gmail was only option back then

2012-2013 @ [redacted] [redacted] VERY specific about email  
record.

no explicit conversation @ DOR

Banner on computer  
Always assumed Hana [redacted] assumed was for  
the record. no more [redacted]

POEMS - on poems

[ When sent to Jake, Hana, Mike had no idea would  
be forwarded to HC.

Everyone in a while received emails about  
system being hacked. Don't recall timing but  
someone from POEMS would talk to someone.  
No specifics

4-10-2011 email

email result of UCLASS email [redacted] from OPS center.  
could be @ home or @ work.

① Strip trail of email - who sent it, etc.

b6  
b7C

So Hana, Jake, Alice just get facts.

clean & make pretty

May have fixed spelling.

S-ESO.

probably put word (Important)

probably came from [redacted]

(SES=0

person's account S-ESO (cc'd)

OPS  
Executive  
Secretary

Jie Mallam

often times would get stuff from ops didn't push forward. or would brief orally.

Not to recreation of ops moving classified up.

Ops Specialist

Watch Fax/Machine hooked up to all of IC.

1 person on shift deals spec. w/ this

"Info comes from everywhere to DoS"

~~Info to specialists~~

Specialists - majority Civil Service

Intensive training - structured training

Most of training @ DoS - field trips

12-14 shifts  
b/4 on own.

INR watch behind SMO

"Thin discussion over email class is healthy.  
think Prob v/ way DoS gathers/uses info"

1A28

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document

33

Date Received 11-23-2015

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

[Redacted]

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned

☐

☒ No

Receipt Given

☐

☒ No

Grand Jury Material - Excluded Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐

Yes

☒ No

Federal Taxpayer Information (FTI)

☐

Yes

☒ No

Reference: Interview Notes

(Communication Enclosing Material)

Description:

☒

Original notes re interview of

[Redacted]

b6  
b7C

1A28

HRC-1178



~~SECRET~~ (U)

UNCLASSIFIED  
U.S. Department of State  
Case No. F-2015-04841  
Doc No. C05739808  
Date: 05/22/2015

STATE DEPT. - PRODUCED TO HOUSE SELECT BENGHAZI COMM.  
SUBJECT TO AGREEMENT ON SENSITIVE INFORMATION & REDACTIONS. NO FOIA WAIVER.

FBI INFO.  
CLASSIFIED BY: NSICG J76J18T80  
REASON: 1.4 (C)  
DECLASSIFY ON: 12-31-2037  
DATE: 11-17-2016

RELEASE IN PART  
B1,B7(D),B7(E),1.4(D),B7(A)

From: Sullivan, Jacob J <SullivanJJ@state.gov>  
Sent: Sunday, November 18, 2012 8:44 PM  
To:  
Subject: FW: FYI - Report of arrests -- possible Benghazi connection

From: Sullivan, Jacob J  
Sent: Sunday, November 18, 2012 8:44 PM  
To: Sullivan, Jacob J  
Subject: FW: FYI - Report of arrests -- possible Benghazi connection

To: Sullivan, Jacob J  
Cc: [REDACTED]  
Subject: FW: FYI - Report of arrests -- possible Benghazi connection

b6 per FBI  
b7C per FBI

*Principal DAS NE*  
This preliminary, but very interesting, please follow. FBI in Tripoli is fully involved.

b6 per FBI  
b7C per FBI

From: [REDACTED]  
Sent: Sunday, November 18, 2012 07:01 PM  
To: Jones, Beth E; Maxwell, Raymond D;  
Subject: FYI - Report of arrests -- possible Benghazi connection

b1 per DOS, FBI  
b3 per FBI  
b7A per DOS  
b7D per DOS  
b7E per DOS

Post reports that Libyans police have arrested several people today who may/may have some connection to the Benghazi attack. They were acting on information furnished by DS/RSC

B7(E)

B7(A)  
B7(E)

1.4(D) (S)  
Overall, B1  
B7(D)

This could lead to something operational, or not, and it could lead to news accounts from Libya saying there is a significant break in the case, or not.

At this point, just FYI.

*A/Dep. Chief of Mission Tripoli  
(probably based on Phone Call)*

Classified by DAS, A/GIS, DoS on 05/22/2015 ~ Class: SECRET/NOFORN ~  
Reason: 1.4(D) ~ Declassify on: 11/18/2032

b6 per FBI  
b7C per FBI

*Spoke nearly every day.*

Department of State

UNCLASSIFIED  
U.S. Department of State  
Case No. F-2015-04841  
Doc No. C05739808  
Date: 05/22/2015

STATE DEPT. - PRODUCED TO HOUSE SELECT BENGHAZI COMM.  
SUBJECT TO AGREEMENT ON SENSITIVE INFORMATION & REDACTIONS. NO FOIA WAIVER.

HRC-1179

STATE: SCB0045788

~~SECRET~~ (U)

11-23-2015

@ [redacted]

b6 per  
b7C FBI

Roles during Sec in office

[redacted]

b6 Per FBI, DOS  
b7C Per FBI, DOS

Sr. Working level expert [redacted]

Main interface through (NEA)  
(CIA) (JASS) A/Sec Feltman (Jeffrey D.)

later Beth Jones

~~Sec~~ Janet Sanderson  
Ray Maxwell

Didnt communicate directly w/ Sec Staff.

Never communicated directly w/ Sec/State

Don't recall comm directly w/ Sec Staff

No w/ Mulls

Maybe 1 or 2 w/ Sullivan.

Separate terminals for unclass v. classified  
on phone every day talking to Amb. Lybia  
talked regularly w/ Amb. (Stevenson) - born open & class  
→ limited classified capabilities  
mobile smart phones.

① Comen early - talk to Stevenster on phone

② brief DAS orally - DAS brief up important info to Asst Sec  
- Sometimes write an email if particularly

questions would come back down through chain of command

Feltman  
or Econ

↓  
J. Sullivan  
C. Mills

No knowledge of external email server  
never received an direct email from Sec of State  
learned when stuff come out in Press

NOV 18, 2012 EMAIL

[REDACTED]

b6  
b7C

briefings usually in AM - email sent in PM  
probably working although Sunday  
but may not have had others in office

If sent to Sullivan assumed forward or brief to  
Sec of State

Re: [REDACTED] contact

everyday would brief contact ↑ via email or orally  
would log in notebook

b6  
b7C

presume

[REDACTED]

got from RSO or Legat/Cairo

Visiting from

SMART system

Didn't archive emails @ DoS

only filing would be when email got full, slide  
over to free up mailbox

~~Don't~~ Congress ~~Don't~~

language in email probably b/c of special circumstances

never used <sup>non</sup> DoS email for work.

Never asked to move from high to low in a way  
that didn't seem right.

Worked w/ Ops Ctr. to set up calls etc.

Couple x a week

Crisis Mgt Group in Ops. during Crisis in Libya

Mgt level

~~SECRET~~ (U)

UNCLASSIFIED  
U.S. Department of State  
Case No. F-2015-04841  
Doc No. C05739808  
Date: 05/22/2015

STATE DEPT. - PRODUCED TO HOUSE SELECT BENGHAZI COMM.  
SUBJECT TO AGREEMENT ON SENSITIVE INFORMATION & REACTIONS. NO FOIA WAIVER.

FBI INFO.  
CLASSIFIED BY: NSICG J76J18T80  
REASON: 1.4 (C)  
DECLASSIFY ON: 12-31-2037  
DATE: 11-17-2016

RELEASE IN PART  
B1,B7(D),B7(E),1.4(D),B7(A)

From: Sullivan, Jacob J <SullivanJJ@state.gov>  
Sent: Sunday, November 18, 2012 8:44 PM  
To: H  
Subject: Fw: FYI - Report of arrests -- possible Benghazi connection

From: Jones, Beth E  
Sent: Sunday, November 18, 2012 02:14 PM  
To: Sullivan, Jacob J  
Cc: [REDACTED]  
Subject: Fw: FYI - Report of arrests -- possible Benghazi connection

b6 per FBI  
b7C per FBI

This preliminary, but very interesting, please see below. FBI in Tripoli is fully involved.

b1 per DOS, FBI  
b3 per FBI  
b6 per FBI  
b7A per DOS  
b7C per FBI  
b7D per DOS  
b7E per DOS

From: Roebuck, William V  
Sent: Sunday, November 18, 2012 07:01 PM  
To: Jones, Beth E; Maxwell, Raymond D; [REDACTED]  
Subject: FYI - Report of arrests -- possible Benghazi connection

AS - DKS

Post reports that Libyans police have arrested several people today who may/may have some connection to the Benghazi attack. They were acting on information furnished by DS/RSC [REDACTED]

B7(E)

B7(A)  
B7(E)

1.4(D)  
B1  
B7(D)

Overall, this could lead to something operationally, or not, and it could lead to news accounts from Libya saying there is a significant break in the case, or not.

At this point, just FYI.

Classified by IAS, AOR, DoS on 05/22/2015 ~ Class: ~~SECRET/NOFORN~~  
Reason: 1.4(D) ~ Declassify on: 11/18/2032

b6 per FBI  
b7C per FBI

Department of State

UNCLASSIFIED  
U.S. Department of State  
Case No. F-2015-04841  
Doc No. C05739808  
Date: 05/22/2015

STATE DEPT. - PRODUCED TO HOUSE SELECT BENGHAZI COMM.  
SUBJECT TO AGREEMENT ON SENSITIVE INFORMATION & REACTIONS. NO FOIA WAIVER.

~~SECRET~~ (U)

HRC-1183

STATE-SCB0045788

[Redacted]

Current: [Redacted]

Former: Director [Redacted]

b6  
b7C

- Introduction

- Voluntary / Can stop at any time
- NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
- FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users. FBI is sensitive to conflicting opinions on the classification of materials – same info from two sources may have different classification levels based solely on the source of the info, i.e., signal vs. diplomatic liaisons.

b6  
b7C

- Brief overview of role(s) between 2/09 and 1/13.

- [Redacted] Guidance on what information is forwarded
- Access to / training on handling of classified information.
  - Guidance on handling classified leaks, or inquiries from press

- Knowledge of the server

- Frequency of emails to / from
- Guidance on sending material to the server
- Procedure for communicating classified information to the Secretary (if applicable)
  - Did it vary when she was traveling, in NY, etc.
- Concerns with the use of the server or other communication channels

- Discussion of specific email(s)

- IClG believed that classified information may be contained in email sent by [Redacted]  
Subject: FYI – Report of Arrest ... sent Sunday, Nov 18, 2011 to multiple parties, forwarded to Sullivan, then to Secretary  
Details surrounding the email chain in question.
  - What was the source of the information cited
  - Knowledge of information being sent to the Secretary
  - Was the information communicated via other channels as well
    - How, Why
  - Typical of other communications made via email?

- Any other thoughts / concerns regarding this matter.
- NDA request

*Handwritten notes:*  
- NEA / A/S  
- DAS.  
- RAY Marshall  
- Sullivan.  
- Beta Jones  
- Sec  
- [unclear]

b6  
b7C

1A29

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

34

Date Received

11/20/2015

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

[Redacted]

b6  
b7C




(SCANNED NOTES - ORIGINALS BEING SENT

VIA DIP PACKET)

1A29

HRC-1185

b6  
b7C

- Introduction
  - Voluntary / Can stop at any time
  - NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
  - FBI's Interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users. FBI is sensitive to conflicting opinions on the classification of materials – same info from two sources may have different classification levels based solely on the source of the info, i.e., sigint vs. diplomatic liaisons.
- Brief overview of role(s) between 2/09 and 1/13.
  - 
  - 
  - 
  - Background on Operations Center
  - Role of Watch Officer/Senior Watch Officer
    - Training
    - Chain of command
    - Guidance on what information is relevant/forwarded
    - How is information pushed forward (verbally/email)
    - Who receives information from the Watch? How?
    - Use of listservs – access to check? Typical delivery?
  - How is watch information documented/archived?
    - Who is responsible? Who has access?
  - Access to / training on handling of classified information.
    - Ever push classified from classified to unclassified?
      - Frequency? Directed? Protocol for doing so?
    - Guidance on press inquiries/leaks of classified information
  - Explanation of "The Line?"
- Knowledge of the server
  - Frequency of e mails to / from HRC
  - Guidance on sending material to the HRC server
  - Procedure for communicating classified information to the Secretary (if applicable)
    - It vary when she was traveling, in NY, etc.
    - If not direct to HRC, who did you email?
    - Extent of interaction/relationship with Huma Abedin, Jake Sullivan, Cheryl Mills?
  - Concerns with the use of the server or other communication channels
- Discussion of specific email(s)

b6  
b7C

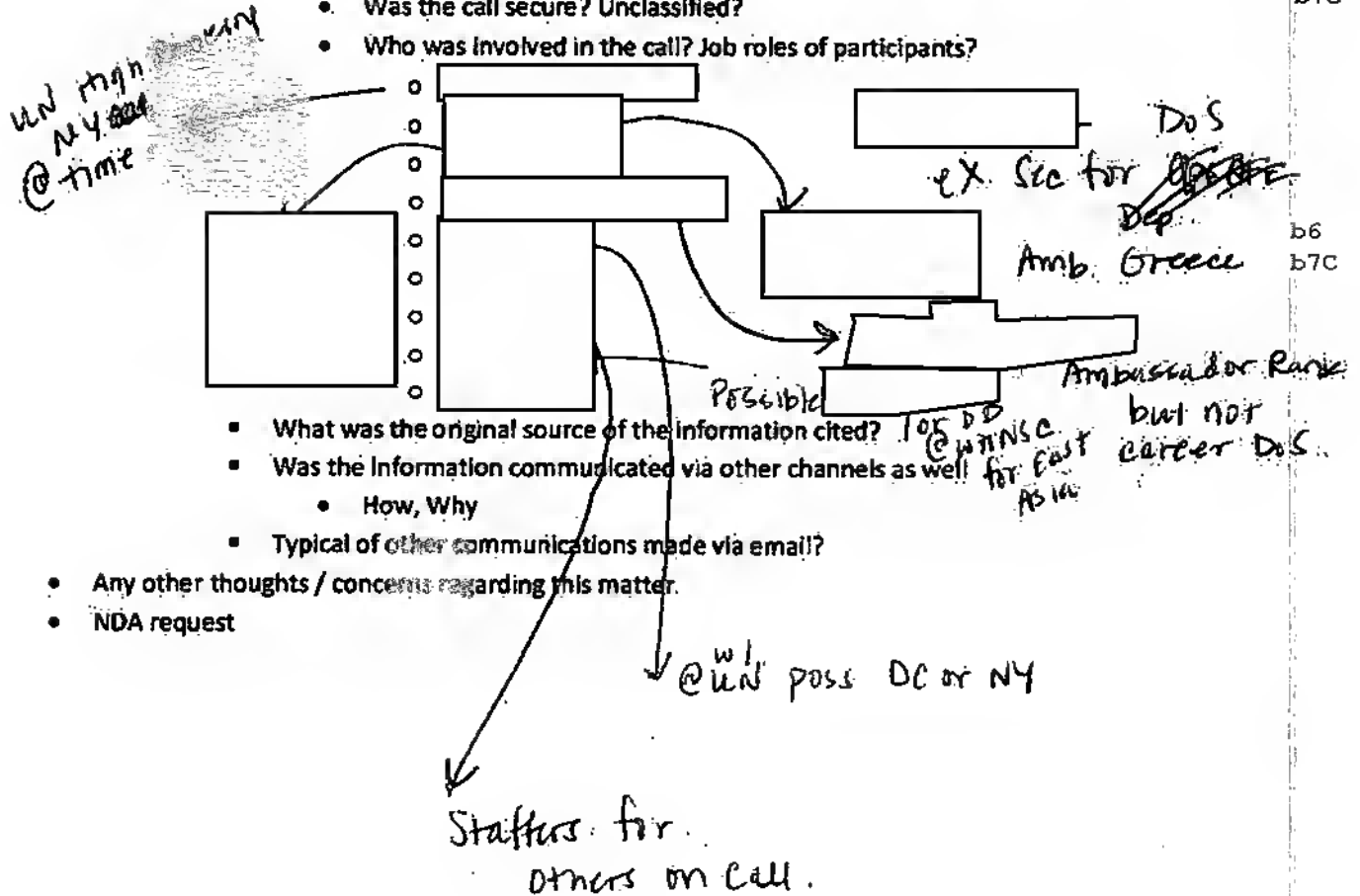


- o ICIG believed that classified information may be contained in email sent by [redacted]  
[redacted] Subject: Summary of 1055 EDT DPRK Conference Call sent Friday, July 3, 2009  
to SES\_DutyDeputies, [redacted] [redacted] S\_Special Assistants, Joseph  
E. Macmanus, and Cc: SES-OSWO-Only, [redacted]

b6  
b7C

- Details surrounding the email chain in question?
- Background on "DPRK conference call"
  - How did you come to learn of the call?
  - How was the call scheduled?
  - Who took notes on the call? [redacted] Is this typical for SWO?
  - Was the call secure? Unclassified?
  - Who was involved in the call? Job roles of participants?

b6  
b7C



b6  
b7C

- What was the original source of the information cited?
- Was the information communicated via other channels as well?
  - How, Why
- Typical of other communications made via email?
- Any other thoughts / concerns regarding this matter.
- NDA request

11-20-2015

@

b6  
b7C

Spot

b6  
b7C

Sr. WO Most Senior

World events

3 shifts

Crisis

Liaison w/ Sec Staff while on travel

Daytime v. Night Shift

7-6 PM  
Bureau of Intel & Res  
INR

Ops Center

Ops  
Center

Crisis Mgt Support

Sr. Watch in Middle

WO Sitt - 1st to answer phone @ cables

after 7PM

Emerg + Stations "hot spots"

7-8 personnel

Ops Specialist - clerical work

fax  
mon

Watch officers

either civil  
service

Comm Affairs WO - comm.

in touch w/ Sec  
Comm's people

or 3rd year

D, p, ec @ time - not sure if still there

Swing station -- extra body on shift during day shift

INR - own operation but present @

SES Duties - Dep. Exec. S [redacted] - Has classification authority  
don't recall if call if Sec [redacted] at  
often on open line  
considering topic

orig reporting came in from other agency prob CIA.  
classified

11p-7a overnight shift.

7<sup>h</sup>-3p

3p-12a

Briefed [redacted] on info Sr. Watch after

b6  
b7c

[redacted] (2 people)

Ops Ctr. log.

not every call logged.

any Sec or D./S. or Under Sec or Asst Sec Log.

archives of cables.

11/20/15

b6  
b7C

b6  
b7C

SR WATCH OFFICER.

- MOST ~~FOR THE~~ ON STAFF (ROTATE)
- 3 SH
- WORLD EVENTS / CRISIS  
FOR ITEMS ON LIST FOR SEC/PRINCIPALS
- "EYES & EARS" FOR SEC
- CO-ORDINATED w/ INTR & CRISIS MGMT SUPPORT
- MORE PEOPLE 7A-7P
- AFTER HRS 7P-6AM 7-8 WATCH OFFICERS
  - MORE JUNIOR PEOPLE
  - CIVIC SERVANTS.

WATCH CENTER - FUNCTION SEC SEC, UNDER SEC,

- SEW OF

- WATCH OFFICER (WU) - <sup>PILOTS, SA</sup>

ASST SEC

- EMERGENCY ACTION OFFICER

- OPS SPECIALIST

- COMM - AFFAIRS OFFICER

- DS OFFICER

- SWING STATION

- INR REP.

CONNECTED TO OTHER  
AGENCIES / OVERSEAS

- NO ANSWERS PHONE

- GATHER INFO & PUSH OUT

- OPEN SOURCE (TV)

- CABLES FROM DOS, CIA, DIA etc

- CABLES - SENT VIA INTERNAL SYSTEMS

- URGENT MATTERS

↳ FLAGGED FOR DIRECTOR OPS CENTER

→ AFTER HOURS - DEPT ASST SEC → TO Sec & Cos

- FOR <sup>URGENT</sup> CLASSIFIED - CALL FIRST FOR GUIDANCE

NEVER EMAILED SEC DIRECTLY (THAT SITE RELAYS)

- EMAILS VIA HOMA

↳ MIGHT ASK FOR A FOLLOW UP CALL ETC

- MASS EMAILS AT HOLIDAYS etc

"FROM Secretary" (presumably STATE ACCOUNT)

- NO KNOWLEDGE OF "H" EMAIL ACCOUNT

# SPECIFIC EMAIL

- WAS ON CALL

Sec. Dty Sec. → Dept. Ex. Sec. → TOLD  
TO CONVEY CALL

- NOT SURE IF IT WAS SECURE CALL OR NOT,

BUT NOT UNCOMMON FOR IT TO BE UNCLASS.  
BK NOT EVERYBODY HAS A SECURE LINE AT RESIDENCE

- EXEC SEC ( [REDACTED] ) FOR DEPARTMENT OF STATE

- NOT ACTIVE PARTICIPANT. → TOOK NOTES,

b6

b7C

FORWARDED TO PEOPLE WHO NEEDED TO  
KNOW BASED ON "CALL SHEETS" plus.

Dept. Ex. Sec. ADD ONS

- CLASSIFICATION REVIEW ~ JUDGEMENT CALL

BY Dept. Ex. Sec., WHO IS AN OCA.

- ORIGINAL REPORTING.

→ SOME AFTER<sup>MS</sup> REPORTING FROM Intel Com

(MAYBE AGENCY) MOST LIKELY CLASSIFIED.

AS CONFIDENTIAL AT THE LEAST

EMAIL UNCLASS, NOT ALL HAVE CLAS ABOARDS, <sup>TYPICAL OF OTHER</sup> COMMS.

0 [REDACTED] - IN NY AT TIMES. High Rank  
U.N. FUNCTION.

b7C

0 [REDACTED]  
0 [REDACTED] - [REDACTED]  
0 [REDACTED]

0 [REDACTED]

0 [REDACTED]

0 [REDACTED] - STAFFERS FOR OTHER  
BUREAUS

0 [REDACTED]

- MAY HAVE BEEN FOLLOW ON DISCUSSIONS  
ON THE NEXT SHEET.

↳ [REDACTED] (SP?) SE W.OFF  
ON THE 4TH

b6

b7C

- 2 SHIFTS IN BTWN [REDACTED]

• WATCH LOG

- ANY SEC CALL, DEPT SEC CALL, UNDER SEC  
AND ASST SEC CALLS, ALL LOGGED

- AND INVOLVED FOREIGN DICTIONARY (GROUPS  
CHIEF  
W-1-B  
B-01)

CLASSIFIED  
MAY HAVE  
SOME  
CONTENT  
NOTES

• NO LOG FOR EQUUS.

• PRINT OR FORWARDED TO 1ST SHIFT

NO OTHER RECORD. SMO EQUUS DISK

LOG ENTRIES INCLUDE:

- PARTICIPANTS.

- TIME.

- SUBJECT / SUMMARY.

## Roles

- WO - ANSWER PHONES, MONITOR CALLS, PUT TOGETHER CALLS, COORDINATE w/ people ON FLOOR TO GET PARTICIPANTS. # OF CALLS DEPENDS ON EVENT. COULD BE ZERO.
- E.A.O. → WATCHES HOT SPOTS, LIAISON w/ CRISIS MANAGEMENT SUPPORT. ~~TO~~ (TASK FORCES)
- SWING → EXTRA BODY DURING THE DAY TO HELP S.W.O.
- Ops Spec → CLERICAL WORK, FAXES, <sup>SEE</sup> COMMS PEOPLE TO GET INFO OUT.
- D.S. → IN HOUSE LIAISON w/ EMBASSIES / RES.
- CONSULAR AFFAIRS OFF → CONSULAR ISSUES AND OTHER AS NEEDED SUPPORT.
- INR - SITS IN BULLPEN BEHIND S.W.O. ARE PLUGGED INTO INTEL COMMUNITY.



1 A30

FD-340 (Rev. 4-11-03)

File Number  302

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 35

Date Received 11/25/2015

From   
(Name of Contributor/Interviewee)

b6  
b7C

1875 Pennsylvania Ave.

(Address)

Washington DC 20006

By SA

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

MIDYEAR EXAM

Reference: 302

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

Property Receipt

Letter provided by Wilmer Hale

1 A30

HRC-1195

COPY  
WILMERHALE

November 25, 2015

[REDACTED]  
National Security Division  
Department of Justice  
Washington, D.C. 20530

[REDACTED]  
b6  
b7C

By Email: [REDACTED]

b6  
b7C

Dear [REDACTED]

Pursuant to our letter agreement with the government dated September 10, 2015, today we voluntarily provided the FBI one black Western Digital brand My Passport Ultra external hard drive, Serial Number WXG1AA3M2130 ("WD Passport Drive"),<sup>1</sup> containing certain data requested by the government. We provided the WD Passport Drive for the purposes of DOJ/FBI's investigation of Secretary Clinton's personal email accounts.

The WD Passport Drive contains the following files:

1. Mr. Cooper's emails<sup>2</sup> to and from Secretary Clinton during her tenure as Secretary of State extracted from a copy of Mr. Cooper's personal and business files from his MacBook Air and MacBook Pro laptop computers.

As you know, we voluntarily provided the FBI with Mr. Cooper's MacBook Air and MacBook Pro on September 24, 2015, and October 5, 2015, respectively. Each machine contained Mr. Cooper's emails to and from Secretary Clinton during her tenure as Secretary of State extracted from email files contained on those machines (along with back-up copies of Secretary Clinton's Blackberry device). Per our agreement with the government, Kroll identified those emails using the spotlight tool that was native to the laptops and worked exclusively on the laptop, i.e., Kroll did not load or use any forensic tools to identify and isolate these emails.

WilmerHale retained a complete copy of Mr. Cooper's personal and business files removed from his MacBook Air and MacBook Pro by creating a "Time Machine" copy of those files. We then reviewed those Time Machine copies using forensic tools and identified Mr. Cooper's emails to and from Secretary Clinton that are contained on the WD Passport Drive. We have securely deleted these emails from the personal and business files retained by WilmerHale.

<sup>1</sup> The WD Passport Drive is encrypted; we provided the password to the FBI.

<sup>2</sup> We treated any email addressed to or from Mr. Cooper as his email. As such, the WD Passport Drive contains not only those emails that were sent between Mr. Cooper and Secretary Clinton but also contains emails that were addressed to both Mr. Cooper and Secretary Clinton (within the same email). This letter refers to such email as "responsive" if it was also dated between January 21, 2009, and February 1, 2013 (Secretary Clinton's tenure as Secretary of State).

November 25, 2015

Page 2

b6

b7c

We believe that we previously produced a majority, likely a vast majority, of the emails on this portion of the WD Passport Drive and that our Time Machine inadvertently captured them as emails that were not produced. Our use of forensic software enabled us to identify, isolate, and remove them from the Time Machine.

2. Mr. Cooper's emails to and from Secretary Clinton during her tenure as Secretary of State, as well as backup copies of Secretary Clinton's Blackberry devices, extracted from an archival image of Mr. Cooper's MacBook Air laptop computer dated December 30, 2013 ("12/30/13 Image").


WilmerHale is maintaining and securely storing a complete copy of all personal and business files removed from the 12/30/13 Image until such time that we reach a written agreement with the government as to what portion we should retain. WilmerHale is also temporarily holding a complete copy of the 12/30/13 Image. We will securely delete that complete copy in seven calendar days from today unless you advise us in writing that the files on the WD Passport Drive are corrupted or that their contents are otherwise irretrievable for reasons that could be cured with the copy we retained.<sup>3</sup>

3. Mr. Cooper's emails to and from Secretary Clinton during her tenure as Secretary of State, as well as backup copies of Secretary Clinton's Blackberry devices, extracted from an archival image of Mr. Cooper's MacBook Air laptop computer dated August 30, 2015 ("8/30/15 Image").

This set of emails includes Mr. Cooper's emails to and from Secretary Clinton during her tenure as Secretary of State extracted from backup copies of Mr. Cooper's Blackberry devices. By comparing MD5 hash values, Kroll determined that other known backup copies of Mr. Cooper's Blackberry devices were forensically identical to those on the 8/30/15 Image. For this reason, as we agreed with the government: (1) Kroll isolated (and we have produced) responsive emails from backup copies of Mr. Cooper's Blackberry devices located only on the 8/30/15 Image; and (2) we are retaining the non-responsive portion of the backup copies of Mr. Cooper's Blackberry devices with responsive emails from only the 8/30/15 Image.

WilmerHale is maintaining and securely storing a complete copy of all personal and business files removed from the 8/30/15 Image until such time that we reach a written agreement with the government as to what portion we should retain. WilmerHale is also temporarily holding a complete copy of the 8/30/15 Image. We will securely delete that complete copy in seven

<sup>3</sup> As you know, we temporarily held images of the MacBook Air and MacBook Pro drives (including files that remained on those machines when they were delivered to the FBI) for the same purpose. You subsequently advised us that the FBI was able to open the files on those machines and we therefore securely deleted those images.

  
November 25, 2015

Page 3

b6  
b7c

calendar days from today unless you advise us in writing that the files on the WD Passport Drive are corrupted or that their contents are otherwise irretrievable for reasons that could be cured with the copy we retained.

As we agreed on September 10, 2015, regarding our consent for the files remaining on the WD Passport Drive:

- We authorize the government to possess and review all of Mr. Cooper's emails to or from Secretary Clinton while she was Secretary of State (January 21, 2009 to February 1, 2013). During that time, Secretary Clinton occasionally sent Mr. Cooper emails for hand-delivery to her husband, President Clinton. We are aware that some of those emails contain information marked "Attorney-Client Privilege."
- We authorize the government to possess the files labeled as back-up copies of Secretary Clinton's Blackberry device. These files do not belong to Mr. Cooper and we therefore lack the authority to consent to an examination of their contents.

We stated in our letters dated September 24, 2015, and October 5, 2015, that Mr. Cooper had not transferred, copied, or retained in any form the files that remained on the MacBook Air and the MacBook Pro. We have since determined that the 12/30/13 Image and the 8/30/15 Image described in this letter contained duplicates of certain files we provided to the FBI on the MacBook Air and MacBook Pro. As noted above, those files are contained on the WD Passport Drive; we will not transfer, copy, or retain those files except as described above. In addition, we have determined that our review/production protocol isolated and produced Mr. Cooper's emails to and from Secretary Clinton, but generally did not lead to us isolating and producing *duplicates* of those emails that were contained in longer chain emails that did not otherwise satisfy the criteria of your request. As you have requested, we are isolating those email chains for production.

Sincerely yours,

b6  
b7c

Enclosures

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T80 NSICG

b6

b7C

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # \_\_\_\_\_

On (date) 11/28/2015

item(s) listed below were:  
☒ Received From  
☐ Returned To  
☐ Released To  
☐ Seized

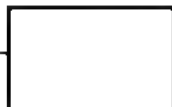
b6  
b7C

(Name) 


(Street Address) 1875 Pennsylvania Avenue NW


(City) Washington, DC 20006

Description of Item(s): One (1) Western Digital My Passport Ultra external hard drive with Serial Number WUX61AA3M2130.



b6  
b7C

Received By:  (Signature)

Received From:  (Signature)

b6  
b7C

1A31

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WFD

Serial # of Originating Document

36

Date Received

12/7/15

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

MID YEAR EXAM.

Reference:

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

EMAIL FROM

[Redacted]

DATED 12/7/15

b6  
b7C

1A31

b6  
b7C

[REDACTED]  
[REDACTED]  
**From:** [REDACTED]  
**Sent:** Monday, December 07, 2015 2:54 AM  
**To:** [REDACTED]  
**Cc:**  
**Subject:** log

[REDACTED]  
For some reason I cannot find your email requesting I look for my phone logs. But I remember that I owe you a response. I have looked through the logs and records I kept. Unfortunately I only kept my notebooks right around and just after the Benghazi incident, i.e., in August and September 2012. I don't have any notebooks for later months. Sorry. Please let me know if there is anything else I can do. Regards, [REDACTED]

b6  
b7C



1A33

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

38

Date Received

12-14-15

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

Washington DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

M. dyer Exam

Reference:

Interview Notes

(Communication Enclosing Material)

Description:

☒

Original notes re interview of

[Redacted]

b6  
b7C

1A33

12-14-15

b6  
b7C

Didnt have access to classified <sup>much</sup> but had clearance. in class side some.

~~in some parts of info~~

In mtgs where classified discussed

No prior  
interaction w/  
He before  
DoS.

① Morning Meeting <sup>3-6 times a week</sup> every day <sup>rarely traveled w/her</sup> He not always there.

② didnt start emailing He until 6-8 mo

① didnt have email so would send to Huma

@ some point He responded direct

§ ☐ asked Huma if okay to go direct

b6  
b7C

"wasnt priv used lightly" - didnt think system was odd. Never in govt before but dealt w/ Gatekeeper system.

when I email today I get back "H" believe before got back "S"

dont recall if PoS or private: dont think it shows.



After review believe info contained in books:

b6  
b7C

5 & 6 showed a bit when re-read.

"Wondering what extent I read... thought through carefully" (before sending up).

[redacted] bold thinker.

b6  
b7C

get idea proposing not revealing  
no idea what she meant by "Marja" Op.

Worked on class system little

[redacted] prob sat entirely on class side

b6  
b7C

don't recall ever a conv. on unclass side that became  
classified / would become confidential (smaller circle)

In opinion - most policy & strateg. "understand people  
participating in conv. might have additional details  
on class side."

Ran development speech for Hc

2011 Email Op Ed

Dont recall ever being instructed not to use personal emails

- used personal laptop
- Dos Blackberry
- Hard to get into Dos system w/ FOB.

- Routine into [redacted] @home  
I would [redacted] back & forth.

b6 per  
b7C FBI

Would get 5<sup>th</sup> emails from Mills - those werent  
Dos account - only one I remember.  
only VERY early

Sullivan always on BB. dont recall ever using  
personal account.

Instructions mostly / think [redacted]  
Dont think I ever

b6 Per FBI, DOS  
b7C Per FBI, DOS

Dos Needs ↑ better technology

~~SECRET~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-17-2016 BY J76J18T80 NSICG

C05759633

CLEAR WITH S/P,  
S/SRAP

CONSULT DOD, CIA

RELEASE IN PART  
B1, B6, 1.4(D)

From: H <hrod17@clintonemail.com>  
Sent: Sunday, September 13, 2009 7:48 AM  
To: 'millsd@state.gov'  
Cc: 'sullivanjj@state.gov'; 'abedinh@state.gov'  
Subject: Re: For S -- for discussion on Afghanistan tomorrow

Yes. Thx.

----- Original Message -----

From: Mills, Cheryl D <MillsCD@state.gov>  
To: H  
Cc: Sullivan, Jacob J <SullivanJJ@state.gov>; Abedin, Huma <AbedinH@state.gov>  
Sent: Sun Sep 13 07:47:17 2009  
Subject: FW: For S -- for discussion on Afghanistan tomorrow

Is this what you are speaking of?

-----Original Message-----

From: Slaughter, Anne-Marie  
Sent: Saturday, September 12, 2009 9:23 PM  
To: Mills, Cheryl D; Sullivan, Jacob J  
Cc: [redacted] Abedin, Huma  
Subject: For S -- for discussion on Afghanistan tomorrow

*talked to every day. Determine what he  
saw & what she didn't*

b6 per  
b7C FBI

I had a long talk with [redacted]

4(D)  
14(D)  
85 (S)

b1 per  
b5 DOS

01231

HRC-1213

~~SECRET~~

~~SECRET~~

C05759633

b1 per  
b5 DOS

(S)

01232

HRC-1214

~~SECRET~~

b6  
b7C

- Introduction

- Voluntary / Can stop at any time
- NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
- FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users. FBI is sensitive to conflicting opinions on the classification of materials – same info from two sources may have different classification levels based solely on the source of the info,

- Brief overview of role(s) between 2/09 and 1/13.

- [redacted]
  - [redacted]
    - [redacted]
      - Frequency and method of communication with the Secretary
  - Access to / training on handling of classified information
    - Guidance on handling classified leaks, or inquiries from press

b6  
b7C

- via Cheryl  
Jare?

- Knowledge of the server

- Frequency of emails to / from
- Guidance on sending material to the server
- Procedure for communicating classified information to the Secretary (if applicable)
  - Did it vary when she was traveling, in NY, etc.
- Concerns with the use of the server or other communication channels

- Discussion of specific email(s)

- ICIG believed that classified information may be contained in email sent by Slaughter (subject "For S – for discussion on Afghanistan tomorrow")
- Details surrounding the email chain in question.
  - What was the source of the information cited
    - [redacted]
  - How did you communicate sensitive / classified information
  - Typical of other communications made via email?

b6  
b7C

- Any other thoughts / concerns regarding this matter.

- NDA request

- Reservations  
about sending  
on unclassified  
system  
when does point  
go from U.S.  
FBI June 03, 2011  
Google email working



- Introduction

b6  
b7C

- Voluntary / Can stop at any time
  - NO NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
  - FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users. FBI is sensitive to conflicting opinions on the classification of materials – same info from two sources may have different classification ~~was~~ based solely on the source of the info,

b6  
b7C

- - - Frequency and method of communication with the Secretary
  - Access to / training on handling of classified information.
    - Guidance on handling classified leaks, or inquiries from press
- Knowledge of the server
  - Frequency of emails to / from
  - Guidance on sending material to the server NO
  - Procedure for communicating classified information to the Secretary (if applicable)
    - Did it vary when she was traveling, in NY, etc.
  - Concerns with the use of the server or other communication channels
- Discussion of specific email(s)
  - ICIg believed that classified information may be contained in email sent by Slaughter (subject "For S – for discussion on Afghanistan tomorrow")
  - Details surrounding the email chain in question.
    - What was the source of the information cited
      -
    - How did you communicate sensitive / classified information
    - Typical of other communications made via email?
- Any other thoughts / concerns regarding this matter.
- NDA request

b6  
b7C

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1353814-0

Total Deleted Page(s) = 11

Page 5 ~ Duplicate;

Page 6 ~ Duplicate;

Page 7 ~ Duplicate;

Page 67 ~ b3 - Per CIA; b6 - Per DOS; b7E - Per DOS;

Page 100 ~ Duplicate;

Page 101 ~ Duplicate;

Page 102 ~ Duplicate;

Page 103 ~ Duplicate;

Page 104 ~ Duplicate;

Page 105 ~ Duplicate;

Page 106 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)       X
X   No Duplication Fee   X
X   For this Page        X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

1A45  
FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

52

Date Received

1/29/2016

From

[Redacted]

(see)

NEW YORK, NY

(Address)

(City and State)

By

[Redacted]

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:



Original notes re interview of

[Redacted]

INTERVIEW NOTES

EMAIL PROVIDED BY

[Redacted]

[Redacted]

1A45

HRC-1351

b3  
b7E

b6  
b7C

b6  
b7C

b6  
b7C

[REDACTED] (WF) (FBI)

b6  
b7C

**From:** [REDACTED]@gmail.com]  
**Sent:** Wednesday, February 03, 2016 10:11 AM  
**To:** [REDACTED] (WF) (FBI)  
**Subject:** [REDACTED] Email Chain  
**Attachments:** February 3 2016 Letter to [REDACTED].pdf

Dear Special Agent [REDACTED]

b6  
b7C

As discussed, attached is the email chain.

Please do not hesitate to contact me with any questions.

Warmly,

[REDACTED]

February 3, 2016

[Redacted]

[Redacted]

Special Agent  
FBI, Washington Field Office

[Redacted]

Dear Special Agent [Redacted]

As discussed, below you will find the email chain we have been discussing. Please do not  
hesitate to contact me with any questions.

Very warmly,

/s/

[Redacted]

b6  
b7C

b6  
b7C

1/29

b6  
b7C

[redacted] joined DOS as [redacted]  
Spec Assist [redacted] then  
[redacted] left in [redacted]  
to join [redacted]

b6  
b7C

- Didn't work directly with HC  
worked w/ Special Assistant w/ the BREAD  
CM, HA (ISS), BP (SECUR) JC (ISS)
- Political Appointee. Sworn in, security briefing  
TS/SGT (NO SAP/COMPARTMENTS), NO FEDERAL  
ACTS OF FOIA TRAINING THAT SHE RECALLS
- Didn't email directly w/ HC until she left DOS  
HROD 17 (until she left)
- Knew she was using a personal account  
Didn't know it was an issue until in the  
press
- Used state gov account when at DOS
- Recalled others using personal accounts  
i.e. [redacted] might forward email from personal  
Account
- Frequently handed class info via Highside
- Don't know how info was transferred from  
[redacted] or JS to HC

b6  
b7C

b6  
b7C

HRC-1357

'NON PAPER'

- NOT FORMALLY SUBMITTED THROUGH THE SYSTEM NOT FOR THE ~~REPORT~~ WORKING PAPER, NOT CUSA ~~BE A MEMO~~
- MAY BE <sup>ON</sup> A VARIETY OF TOPICS
- COULD BE CLASSIFIED

IPAD

- NO KNOWLEDGE OF
- NEVER TRAVELED W/ HC WHILE AT DOS, W/ JS   <sup>BT TRAVEL</sup>
- NEVER AT RESIDENCES. ( " "

PRIVATE OFFICE: AFTER DOS

→  New York

AT HOME TILL

ZFS → LLC OR PRIVATE OFFICE

RESPONSE

- PHONE CALLS ~~REMARKS~~ <sup>REMARKS</sup> ~~ARTICLE~~ <sup>ARTICLE</sup>

+

Monica → PERSONAL ASSISTANT

° NO MEMORY OF EMAILS BEING TURNED OUT  
OR CALLED DOWN

PRN - JAN 2014

= [ ] → WOULD GIVE ADVICE ON IT FOR  
THE TEAM. (INFRASTRUCTURE, BUYING LAPTOPS.)

b6  
b7C

- SPOKE FREQUENTLY
- I.E. <sup>SHOULD WE!</sup> GOOGLE BUSINESS, CLOUD BASED MS OFFICE, etc

LAPTOP.

= SPOKE W/ MONICA APPROX 1 MONTH AGO.

= NO RECOLLECTION OF RECEIVING IT.

= [ ] WAS THE MAIN RECEIVER OF MAIL BUT

b6  
b7C

WOULDN'T OPEN IF IT WAS ADDRESSED TO [ ]

\* - HAS EMAILS W/ MONICA RE: ARCHIVE EFFORT, <sup>FEB/MARCH 2014</sup>

WILL PASS LAPTOP TO YOU.

= MAYBE A MAC?

\* - OCCURRED WHILE WORKING AT HOME WAS  
PROBABLY SENT TO THE FOUNDATION, NOT  
SURE HOW IT WOULD HAVE BEEN HANDLED IF  
NOT ADDRESSED TO HER

HACKS

RECALLS CYBER SECURITY AGENTS RE: PLC  
HACKING ACCOUNTS.



hrod17@

[redacted]

b6  
b7C

NY [redacted] - worked from home [redacted]

2FS -

[redacted]

b6  
b7C

Executive Asst. / P  
briefing memos.

Huma cos.

[redacted]

- April / May 2014  
DD Sched.

b6  
b7C

Monia Valmore - Sched.

[redacted]

[redacted]

PRN frequent

- Jan 2014 - July 14

NY  
Office

[redacted]

b6  
b7C

gave advice on  
IT Infrastructure

Cloud base

Mac  
1 March  
Feb 2014  
Spoke April

↓ Mar!

Monia called 1-2 mo ago.  
during period

Foundation

Sometimes take mail

~~SI/NTF~~

1A46

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

202

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 53

Date Received 2-8-2016

From Steven Mull

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Midyear Exam

Reference: Interview Notes: Re Mull

(Communication Enclosing Material)

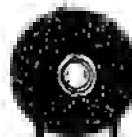
Description: ☒ Original notes re interview of Mull

1A46

~~SI/NTF~~

HRC-1361

~~S/10/1F~~



~~S/10/1F~~

Mu

CE

2-1-16

2009-13

June 10 - Oct 12 - Executive Sec

June '10 - Sr. Advisor to Sec Pol Affairs

2012 - Aug 2015 - Amb Poland

↓  
In charge of entire ex secretarial / in support of Sec Pos.  
Most interaction w/ Mills HRC Ctr.

① Formal info processing to from Sec of State / OPS Ctr

② crisis mgt.

pull together TF to manage crisis on behalf of Sec Pos

③ support of travel - mng reporting (Mobile Comm)

④ IT support / Mobile # in office / all sr. principals  
POEMS.

Didn't really know if personal email was common for  
Sec of State.

Informal v. Formal comm.

Sec asked Muell to look into MILK or Aumai.  
IPAD use. - early

Re: Email "I think it was iPad"

Couldn't do b/c space.

Security personnel

b6  
b7c

Ne [redacted] He usi [redacted] mobile device in a  
just famous pic of BB on plane. don't think  
prohibition about it

Re: Email w/ HA about Issuing Dos BB

Set up terminal (usually)  
normal means of comm not working so asked  
for BB. from Exec. Sec.

told any comms subj to FOIA b/c DoS device  
HA responded decided against.

Not aware He ever issued Dos BB or elect<sup>Port</sup> device

Don't know who responsible for maintaining device  
or making sure within Dos policy

Bluetooth vulnerabilities Email

Sec officer [redacted] - wanted 7th floor [redacted] be aware  
of vulnerabilities w/ BB or bluetooth  
not sure what prompted

b6  
b7c

Strike in  
2011

Concern private email accounts hacked

J. Sullivan

Heard from [redacted] private emails compromised

b6  
b7c

Everybody in the office on PDENS. Except HC.  
Staff usually used PDENS. How full comm w/ them.

Assume blue tooth. Cap on. So devices disabled.

the private device not before swap out.

MComm team -

b6  
b7C

Sec.  
for the office

John Bentel head of PDENS

(Tuli)

Mushingi

Now  
Amb Nogadug  
Burkina Faso

Deputy for Admin Support  
Direc Sup Mob team

Ambassador Stephen Mull  
Executive Secretary (2011)

[redacted] // Telephone [redacted] Office Manager [redacted]

b6  
b7C

- Introduction

- o Voluntary / Can stop at any time ✓
- o NSLB Disclaimer re: Garrity / not interested in prior statements to DOS ✓
- o FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users.

- Brief overview of duties as the Executive Secretary

- o What were your duties as they related to the operation of the Secretary's private server, or other mobile comms platforms?
- o What were your duties as related to the Ops Center?

- Knowledge of the private server and email

- o Was there an approval process for the use of private email / email servers?
  - If so, what is the approval process for this arrangement?
  - What steps were taken to review the risks / benefits of this arrangement?
  - Who was involved in the review process?
  - Was this consistent with DoS policy at that time?
  - Did the server violate department policy as stipulated in the Foreign Affairs Manual?
  - What is the current policy today?
    - When / why did it change?

- o Who had knowledge of the server from DOS at the onset?

- When did you become aware of the arrangement?

- o Did DOS have any role in setting up and / or maintaining the server?

- If so, who specifically was responsible for this? ? don't know

- DoS employee, or a contractor?

- o If contractor, what steps to ensure actions were consistent with IMS-POEMS procedures, protocols?

- o If contractor, what steps to ensure appropriate threat monitoring?

- o Knowledge of Brian Pagliano's role? Payment structure?

- What steps were taken to ensure appropriate security protocols were in place (updates, patches, antivirus, intrusion monitoring)?

- Who paid for the set up costs and maintenance costs?

- Were the secretary's server related expenses reimbursed by State?

- o If paid for by State, what is the policy on paying for the maintenance of personal property?

- o What guidance was provided by DoS regarding the transmission / storage of sensitive and/or classified information on the server?

- What secure comms were available to the secretary at her home and when she was traveling?
  - Phone
  - Fax
  - Email (Classnet / JWICS)
- Discussion of emails
  - August 2011 email regarding state issued BB (connectivity issues following hurricane Irene)
  - November 2010 email regarding Bluetooth vulnerabilities (CLASSNET – SECRET)
    - Why was this sent to Cheryl? (i.e., was it requested, was it standard to send such alerts, etc)
    - Did they request the offered briefing / demo?
    - Were the implied recommendations to disable Bluetooth implemented?
      - By whom?
      - Who maintained her blackberry w/ respect to security etc
        - Did you have direct contact with them? How often?
        - Did they request information about DoS security recommendations? How often?
  - July 2010 Email (use of mobile device in office)
    - Background context on this?
    - What device are they referring to (ipad)?
    - What was the resolution – was she able to use it in her office?
      - Did she use other devices in her office?
    - Who else was involved in these discussions / approvals
- Any other thoughts / concerns regarding this matter.
- NDA request



**From:** "Macmanus, Joseph E" <CLASSSTATE/CBPC ADMINISTRATIVE GROUP/RECIPIENTS/MACMANUSJE>  
**Sent:** 10/6/2009 6:07:49 PM +00:00  
**To:** "Mills, Cheryl D" <MillsCD@state.sgov.gov>; "Sullivan, Jacob J" <SullivanJJ@state.sgov.gov>; "Abedin, Huma" <AbedinH@state.sgov.gov>  
**Subject:** IT security in Moscow

Our Mobile Communications Team sent in an email on electronic surveillance and monitoring in Russia, which I've excerpted below. The gist of it is: what's yours is theirs.

We will brief staff at the airport before departure, and post the necessary warnings in the hotel.

**From:** Mobile Communications Team, Moscow Advance  
**Sent:** Tuesday, October 06, 2009 10:40 AM  
**Subject:** IT security in Moscow

b7E Per DOS

Yesterday at the RSO's security briefing, the RSO stated that the IT threat level here in Moscow currently [REDACTED]

**The following are recommendations regarding IT security in Moscow:**

b7E Per DOS

Strong recommendation against any classified material or conversations in the hotel, including STE conversations and any printed materials, whether brought to the hotel by the party or delivered by courier. No matter how well [REDACTED]  
[REDACTED] The Secretary's suite as well as the Senior Bureau, the Secretariat, and all bedrooms will be [REDACTED]

b7E Per DOS

[REDACTED]

Strong recommendation against the use of BlackBerries: when you bring your BlackBerry online in Moscow, [REDACTED]

[REDACTED]

Strong recommendation against computers connected to the Internet in the hotel,

[REDACTED]

b7E Per DOS

Authorized the use of FOBs in the hotel ONLY for use with government-owned laptops under 100% continuous positive control by a cleared American. If left unattended at any time, for example, while somebody goes downstairs for breakfast, they will be compromised.

NOTE: a lost or stolen FOB here in Moscow is a major security threat. All must take great care not to loose their FOBs. [REDACTED]

[REDACTED]

b7E Per DOS

DS Lead and DS Logistics indicated that they did not want computers and printers in their bedrooms per the IT requirements and would rather work in the Embassy. The laptops intended for them are being stored in the Embassy.

**Communications set-up in Moscow:**

Computers issued by MCT or supported by MCT (e.g., Abedin, Sullivan, Macmanus) will [REDACTED]

b7E Per DOS

[REDACTED] the Marines and DS will restrict access. Anyone in a bedroom outside of the [REDACTED] must keep their laptops in their possession at all times

store them at the Embassy (for example in [REDACTED])

b7E Per DOS

Computers we set up in S offices and bedrooms will be laptops owned by the Embassy and will remain in our custody while outside of the Embassy. The traveling party should be notified that we will have to use laptops instead of desktops at this stop.

STEs in the S suite: the Secretary should be briefed [REDACTED]

b7E Per DOS

RSO recommends courier of documents to the hotel [REDACTED]

b7E Per DOS

RSO permits use BlackBerries. AS SOON AS users return to Washington, their Blackberry will need to be cleaned [REDACTED]

b7E Per DOS

Any government laptop used in the hotel and returned to Washington will need to be [REDACTED]

b7E Per DOS

The use of a personal computer is not recommended; [REDACTED]

b7E Per DOS

---

**From:** "Abedin, Huma" <SBUSTATE/SES/RECIPIENTS/ABEDINH>  
**Sent:** 8/30/2011 9:34:07 PM +00:00  
**To:** "Mull, Stephen D" <MullSD@state.gov>  
**Subject:** Re: S Communications

Its pretty silly and she knows it.

---

**From:** Mull, Stephen D  
**Sent:** Tuesday, August 30, 2011 05:18 PM  
**To:** Abedin, Huma  
**Subject:** RE: S Communications

Thanks for reminding all of this very helpful context!!! ☺

---

**From:** Abedin, Huma  
**Sent:** Tuesday, August 30, 2011 17:17 PM  
**To:** Mull, Stephen D; Mills, Cheryl D  
**Cc:** Kennedy, Patrick F; Hanley, Monica R  
**Subject:** Re: S Communications

Steve - let's discuss the state blackberry, doesn't make a whole lot of sense.  
As for the equipment, the commo team was limited in some capacity because we did not have authorization from owners of residence to install equipment. We did it regardless. Additionally, as S knows, the team didn't have access to the property until a couple of hours before S arrived. Finally, as even the white house attested, this was a pretty wide spread problem, not just affecting us. So we should bear that in mind.

---

**From:** Mull, Stephen D  
**Sent:** Tuesday, August 30, 2011 01:39 PM  
**To:** Mills, Cheryl D  
**Cc:** Abedin, Huma; Kennedy, Patrick F; Hanley, Monica R  
**Subject:** S Communications

Cheryl,

Thanks again for alerting me to the communications issues the Secretary has been having. Here's a status report:

- On the immediate problem of the Secretary's not being able to have her calls transferred, [REDACTED] b7E Per DOS  
[REDACTED]  
[REDACTED] technicians are onsite now [REDACTED]  
[REDACTED]

- On the more long-term issue, I've asked our team to develop an enhanced package of capabilities and equipment that we would be deploying with the Secretary to be as closely co-located as possible with her when she is on travel away from her usual residences. The package will include things that anticipate the normally unexpected such as hurricanes, power outages, earthquakes, locusts, etc, such as generators, uninterrupted power supplies, supplementary satellite capabilities, including satellite phones for when local infrastructure fails (as it did in NY over the weekend).

Separately, we are working to provide the Secretary per her request a Department issued Blackberry to replace her personal unit which is malfunctioning (possibly because of her personal email server is down). We will prepare two versions for her to use — one with an operating State Department email account (which would mask her identity, but which would also be subject to FOIA requests), and another which would just have phone and internet capability. We're working with Monica to hammer out the details of what will best meet the Secretary's needs.

Please let me know if you need anything more for now, and I'll be in touch with the above longer term options soon.

Thanks,

Steve

-----  
PR\_RIM\_MESSAGE\_SUBMISSION\_ID:

[REDACTED]

PR\_RIM\_PAGER\_TX\_FLAG:

true

b7E Per DOS

PR\_RIM\_INTERNET\_MESSAGE\_ID:

[REDACTED]

PR\_RIM\_MSG\_FOLDER\_ID:

-5

PR\_RIM\_MSG\_REF\_ID:

876690920

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 03-23-2019 BY C66W46B11 NSICG

From: "Mull, Stephen D" <CLASSSTATE/CIISNPM/RECIPIENTS/MULLSD>  
Sent: 11/9/2010 4:32:28 PM +00:00  
To: "Mills, Cheryl D" <MillsCD@state.sgov.gov>  
Subject: FW: FW: Bluetooth Vulnerabilities

Hi Cheryl,

Here's the summary of Bluetooth vulnerabilities I mentioned. If you'd still like a briefing/demo (which I think you'd find pretty interesting/disturbing), let me know and I'll be happy to set up. Not that I normally like to disturb my boss!

Steve

From: Bentel, John A  
Sent: Friday, November 05, 2010 4:23 PM  
To: Mull, Stephen D  
Cc: Lukens, Lewis A; Green, Milton V; Jacks, Yvette R  
Subject: Bluetooth Vulnerabilities

Steve:

Listed below are vulnerabilities of Bluetooth on a Blackberry. Further down you will find more technical details should you wish to read more.

At the recommendation of our IT counterparts in DS - I have reached out to DAS Gentry Smith requesting to meet to see if it is possible to enable Bluetooth and adhere to a security posture.

Please let me know if you have any questions or concerns. Will keep you posted.

Thanks,

John

(S/NC)

Can be exploited from a considerable distance away and be undetected.

Attacker can take full control of the device.

Attacker can take every email on the device.

Attacker can set up an attack to move to any new device swapped out using the same SIM.

Attacker can listen to any phone conversation.

Attacker can turn the phone into a listening device.

Able to use the phone to send SPAM emails looking as the user.

Expanded details follow:

Biggest concern to the agency:

- o During the August 2009 DEF CON (the Annual Las Vegas "hacker convention"), a computer security consultant discovered an unauthorized path into corporate information networks - using the BlackBerry. The consultant developed a hacking program exploiting the trust relationship between the BlackBerry and a company's internal BES server. Because the data tunnel between the BlackBerry and the server is encrypted, intrusion detection systems at the perimeter of the network will not detect the attack. The technique is also possible because many companies are not equipped to detect someone trying to deliver an exploit from inside a network. This is true because they view the BlackBerry as a plausible attack vehicle.

The first exploit is known as "BLUESNARFING". ALTHOUGH BLUETOOTH IS WIDELY CONSIDERED A SHORT RANGE NETWORK STANDARD, THE EFFECTIVE RANGE OF THIS ATTACK CAN BE EXTENDED WITH HIGH GAIN ANTENNAS UP TO A MILE.

A GREATER THREAT INVOLVES WHAT IS REFERRED TO AS A "BLUEBUG" EXPLOIT, WHERE THE ATTACKER TAKES REMOTE SERIAL ACCESS TO THE DEVICE AND THEREBY GAINS FULL CONSOLE CONTROL. THIS ALLOWS THE ATTACKER TO DO THE FOLLOWING:

- > MAKE TOLL FREE CALLS
- > CHANGE ANY AND ALL PHONEBOOK ENTRIES TO A RECORD AND FORWARD NUMBER TO MONITOR CONVERSATIONS
- > HACK/SEND SPAM EMAILS FROM A TARGET'S PHONE
- > HAVING SOMEONE'S PHONEBOOK WOULD ALLOW AN ATTACKER TO NAMEDROP AND SOCIALLY ENGINEER THE TARGET TO DISCLOSE SENSITIVE INFORMATION
- > TURN A PHONE INTO AN OPEN MICROPHONE BY CONFIGURING IT TO AUTOANSWER AN INCOMING CALL WITHOUT RINGING
- > LISTEN TO THE TARGET'S VOICEMAIL

READ OR SEND TEXT MESSAGES TO OR FROM THE TARGET, RESPECTIVELY.

The "BACKDOOR" attack creates a secret paired (authenticated) relationship between a target device and a rogue device, allowing trusted connectivity and compromising the target's local data and services. Some Bluetooth-equipped cell phones, for instance, don't erase their lists of paired devices when users' Subscriber Identity Module (SIM) cards are swapped, enabling this type of attack to be moved from one device to another.

The "BLUEJACKING" technique involves abusing the bluetooth "pairing" protocol, the system by which bluetooth devices authenticate each other. The technique uses the first part of the process that allows the exchange to take place, and is therefore open to further abuse if the handshake completes and the "bluejacker" successfully pairs with the targeted device. If such a pairing occurs, then all data on the target device becomes available to the Initiator. This includes every mail stored on the device.

~~Sensitive~~

This email is UNCLASSIFIED.

Message Headers:



b6 Per DOS

Date: Tue, 9 Nov 2010 11:32:28 -0500



b6 Per  
b7E DOS

From: "Mull, Stephen D" <MullSD@state.sgov.gov>  
To: "Mills, Cheryl D" <MillsCD@state.sgov.gov>

Classification:  
SensitivityCode:  
AttachmentsClassification:  
SMARTClassificationData:

UNCLASSIFIED  
~~Sensitive~~

**From:** "Mull, Stephen D" <SBUSTATE/CIISNPM AG/RECIPIENTS/MULLSD>  
**Sent:** 7/7/2010 12:37:35 PM +00:00  
**To:** [REDACTED]  
**CC:** "Abedin, Huma" <AbedinH@state.gov>  
**Subject:** RE: HRC

b6 Per  
b7C DOS

See you then!

-----Original Message-----

**From:** [REDACTED]  
**Sent:** Wednesday, July 07, 2010 08:37 AM  
**To:** Mull, Stephen D  
**Cc:** Abedin, Huma  
**Subject:** Re: HRC

b6 Per  
b7C DOS

Great, I'll swing by at 12:30

----- Original Message -----

**From:** Mull, Stephen D  
**To:** [REDACTED]  
**Cc:** Abedin, Huma  
**Sent:** Wed Jul 07 08:32:22 2010  
**Subject:** RE: HRC

I am; either time works.

-----Original Message-----

**From:** [REDACTED]  
**Sent:** Wednesday, July 07, 2010 08:06 AM  
**To:** Mull, Stephen D  
**Cc:** Abedin, Huma  
**Subject:** Re: HRC

b6 Per  
b7C DOS

Steve are you by chance free either at 12:30, or 2pm?

-----Original Message-----

**From:** [REDACTED]  
**To:** Mull, Stephen D  
**Cc:** Abedin, Huma  
**Sent:** Thu Jul 01 11:33:11 2010  
**Subject:** Re: HRC

Will do

b6 Per  
b7C DOS

----- Original Message -----

**From:** Mull, Stephen D  
**To:** [REDACTED]  
**Cc:** Abedin, Huma  
**Sent:** Thu Jul 01 11:29:08 2010

HRC-1375



Subject: RE: HRC

Sure [redacted] that would be great, though we should probably talk first in person before involving others. Just let me know when's convenient for you when you get back.

b6 Per  
b7C DOS

-----Original Message-----

From: [redacted]  
Sent: Thursday, July 01, 2010 09:58 AM  
To: Mull, Stephen D  
Cc: Abedin, Huma  
Subject: HRC

Hey Steve,

Hope you're settling in to the nicest office at HST. When we're back from Europe, I'm hoping to sit with you and not sure who else is relevant. HRC wants to use an electronic device we bought for her in her office, wants me to figure out if it's doable or what we have to do to make it doable. I don't know who replaced Julia Hill, but I assume they should sit in too, maybe Cindy Almodovar who I think is the best IRM person in the department.

[redacted]

b6 Per  
b7C DOS

-----  
**Message Headers:**

b6 Per  
b7E DOS

From: "Mull, Stephen D" <MullSD@state.gov>  
To: "Reines, Philippe I" <reinesp@state.gov>  
Cc: "Abedin, Huma" <AbedinH@state.gov>

HRC-1376

PR\_RIM\_INTERNET\_MESS

AGE\_ID:

PR\_RIM\_MSG\_STATUS:

PR\_RIM\_MSG\_DN\_DEVICE

\_3\_6:

PR\_RIM\_MSG\_REF\_ID:

PR\_RIM\_MSG\_FOLDER\_ID:

[REDACTED]

state.sbu>

0

true

-1139874124

-6

b6 Per  
b7E DOS

PR\_RIM\_MESSAGE\_SUBMI

SSION\_ID:

PR\_RIM\_DELETED\_BY\_DE

VICE:

PR\_RIM\_PAGER\_TX\_FLAG:

[REDACTED]

true

true

b7E Per DOS

1A47

FD-340 (Rev. 4-11-03)

File Number [redacted] - 302

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 54

Date Received 2-3-2016

From [redacted]  
(Contributor/Interviewee)

b6  
b7C

(Address)

Washington DC  
(City and State)

By [redacted]

b6  
b7C

To Be Returned ☐ Yes ☒ No  
Receipt Given ☐ Yes ☒ No  
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure  
☐ Yes ☒ No  
Federal Taxpayer Information (FTI)  
☐ Yes ☒ No

Midyear Exam

Reference: Interview of [redacted]  
(Continuation Enclosing Material)

b6  
b7C

Description: ☒ Original notes re interview of [redacted]

b6  
b7C

1A47

HRC-1378

[redacted] Video Transcript

[redacted] Clinton Admin

b6  
b7C

In context as to what changed  
Video quote: since last admin

margins  
made how  
we transmit  
more  
instantious

b6  
b7C

[redacted] - Not classified.

just the substance of how you do work.

[redacted] Clinton Admin

No way to have access to  
unclass systems.

would communicate via cables.

① Is it classified  
② Is it affecting  
Sources & Meth.

b6  
b7C

When return.

SIPR  
JWicks.  
unclass  
Blackberries / unclass  
iPad (Secure)

turned over personal.  
email from Gmail for  
FOIA.  
that related even closely  
to work.

DD FBI - anecdote:

[redacted] (cell)

b6  
b7C

[redacted]

- Introduction
  - Voluntary / Can stop at any time
  - NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
  - FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users.
  - Witness identifiers, 3<sup>rd</sup> party witnesses and affect on confidentiality
- Brief overview of duties as [redacted]
  - Clearance, training, frequency of handling classified information
- Knowledge of the private server and email
  - When did you become aware that the Secretary was using a private email / server?
  - Was this consistent with DoS policy?
  - Did you ever witness the email content that you felt was particularly sensitive even if it wasn't marked as classified?

b6  
b7C

- Discussion of video
  - [redacted] 2013 speech to the American Foreign Service Association

b6  
b7C

[redacted]

Video quote:

[redacted]

b6  
b7C

- Can you provide some context to this statement?

- What did [redacted] mean by [redacted]  
[redacted]
  - Was sensitive or classified information conducted on the system?
    - In this instance or ever?
  - Was [redacted] classified? – No
    - How would this be crafted pre-BB? Why?
- When does US strategy / policy or other diplomatic negotiations become classified in your mind?

b6  
b7C

b6  
b7C

- Any other thoughts / concerns regarding this matter.
- NDA request

[redacted] 2-3-2016.

b6  
b7C

w/ [redacted]

b6  
b7C

@ DOS.

b6  
b7C

~~TS/SCT~~

& some compartments.

Everyday dealt w/ classified

PDB Everyday  
Recipient.

b6  
b7C

Paper - to Secretary re: classified / on Mahag. Row.

No idea of personal account.

Don't recall what saw when email from HRC came up.

Nobody in DOS uses a device w/o approval.

my assumption was whatever device she used was  
approved.

Not aware of DOS policy against use of private email.  
Traveled a few times w/ Sec of State.

If classified by ~~secure~~ telephone

who? → or by secure media / computer

think misconception about classification of documents  
only way to talk w/ foreign partners was via  
email. & I'm sure later classified

Hack — I'm sure people tried to hack accounts of  
team.

b6  
b7C

just  
before  
negotiations  
2 yrs ago

traced back to Turkish server  
DS.



FD-340 (Rev. 4-11-03)

1A48

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

55

Date Received

FEB 10, 2016

From

[Redacted]

(Interviewee)

b6  
b7C

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

[Redacted]

b6  
b7C

1A48

HRC-1384

2-10-2016

b6  
b7C

885 3<sup>rd</sup> Ave NY

b6  
b7C

b6  
b7C

Reading Review/Memo  
Controlling Info Flow.

Informal & Formal Mtgs w/ DOS.

PCM - Principal Comm Meetings <sup>deputy</sup> DCM  
Coordinate packages. / coordinate w/ Counterparts

PCM - few x week 0-4

DCM - 3-5 x week.

C DOS contacts. J. Sullivan  
Joe McMannus.

3 computers on desk  
unclass, SIPR, Jwics.

Weekly Inouch / Separate.

Sec Gates  
Donlon  
Clinton

3 phones  
2 class, 1 regular

not



position

b6  
b7c

Archiving functioning [redacted] NSC Executive Secretary.

- ↑
- Know Jack Sullivan from prior Govt. service

[redacted] Interview Outline

Professional Background

- [redacted] - current)
- [redacted] at DoD [redacted]
- National Security Council [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

Question Outline

- Introduction
  - FBI's interest in the matter
  - NSLB disclaimer re: prior statements
  - Can consult counsel if necessary
- What is your current position?
- Brief description of role at NSC as relative to Department of State?
  - How often did you coordinate with DoS?
    - For what types of matters?
    - Who were your primary contacts at DoS?
    - What was the nature of the communications?
    - How often did you send / receive documents to DoS?
      - Examples of?
        - Classified, unclassified?
        - How were the documents transferred?
- Email regarding PC meeting
  - October 4, 2009 email chain with [redacted] regarding content for a Restricted PC meeting on October 5<sup>th</sup>, 2009 regarding Af-Pak. [redacted] recommendations - [redacted]
    - Do you recall the Restricted Principals Committee meeting? Can you provide general context on who / what was involved?
      - Do you recall if the final product for the PC meeting was classified?
        - At what level(s)?
    - EMAIL 1 -
      - What is being couriered and to whom?
        - Is this typical?
      - What is at the Secret level?
      - What is the DNI stuff that you are referring to? What was it classified?
        - Where did you get it from?
        - How can we track it down?
    - EMAIL 2a, 2b and 3 -
      - What was the 'DNI piece' specifically?
      - Who was the originating agency?
      - What was the classification of the piece?
      - Where was it couriered to, DOS? How would this have been done? Who would have sent it / who would have it been sent to?
    - EMAIL 4 -

*Evac. spec! ...*  
*PC - 0-3H/WK.*  
*DC - 3-5+/WK.*  
*Former*  
*informer.*  
*- WKly Council.*

b6  
b7C

b6  
b7C

- What is the standard procedure for distro of the package. Who does it go to?
- **EMAIL 5 –**
  - What is washfax?
- **EMAIL 6 –**
  - What does Tab 2 refer to specifically?
    - Is it the same as the 'DNI piece' referenced above?
    - What was the classification level of this doc, TS?
      - DNI piece appears to be S, as you attempted to send it via SIPR
    - Does NSC / EOP archive content from each PC meeting?
      - What department / who is the POC for this?
- **EMAIL 7 –**
  - Were there any follow up items?
  - What would typically happen after a PC meeting with regards to specific policy / strategy?
  - How would decisions from the meeting be disseminated to relevant agencies?
- **EMAIL 8 & 8a – (header / footer email – to on way forward in Afghanistan, Plan for PC tomorrow, meeting with Clinton and Petraeus)**
  - What was the context of this email?
  - Do you recall what supporting information was provided by DoS
    - Classification of it?
    - Is it maintained by NSC.
- Did you ever have concern about the transmission of sensitive / classified info on unclass, or non-government?
- Any other relevant information?
- NDA

1st cut DC  
 2nd cut AC  
 3rd cut J  
 4th cut KISC  
 5th cut

[redacted] Interview Outline

b6  
b7c

Professional Background

- [redacted] - current)
- [redacted] at DoD
- National Security Council [redacted]
- [redacted]
- [redacted]

Question Outline

- Introduction
  - ✓/o FBI's interest in the matter
  - ✓/o NSLB disclaimer re: prior statements
  - o Can consult counsel if necessary
- What is your current position?
- Brief description of role at NSC as relative to Department of State?
  - o How often did you coordinate with DoS?
    - For what types of matters?
    - Who were your primary contacts at DoS?
    - What was the nature of the communications?
    - How often did you send / receive documents to DoS?
      - Examples of?
        - o Classified, unclassified?
        - o How were the documents transferred?
- Email regarding PC meeting
  - o October 4, 2009 email chain with [redacted] regarding content for a Restricted PC meeting on October 5<sup>th</sup>, 2009 regarding Af-Pak [redacted] recommendations - [redacted]

b6  
b7c

ways to cour. to DoS

- ① Wash Fax - Secure Fax
- ② courier.

EMAIL 1 - Don't have rec. of specific Mtg. - Asking for papers frequent.

- What is being couriered and to whom? Not sure
  - o Is this typical?
- What is at the Secret level?
- What is the DNI stuff that you are referring to? What was it classified?
  - o Where did you get it from?
  - o How can we track it down?

Don't recall specific

EMAIL 2a, 2b and 3 -

- What was the 'DNI piece' specifically?
- Who was the originating agency?
- What was the classification of the piece?
- Where was it couriered to, DOS? How would this have been done? Who would have sent it / who would have it been sent to?

EMAIL 4 -

Don't recall  
this particular DNI  
assessment.

In PC & DC principals provided w/ packet before.

LC paper  
DOS paper

DDD paper

→ Sent out ahead to HRC-1389  
digest

Regular chann.

① NSC sends Mtg. notice  
& request for packages.  
Pac. come in 3-4 days by

- What is the standard procedure for distro of the package. Who does it go to?

▪ EMAIL 5 -

- What is Washfax? Secure

▪ EMAIL 6 -

- What does Tab 2 refer to specifically?
  - Is it the same as the 'DNI piece' referenced above?
  - What was the classification level of this doc, TS?
    - DNI piece appears to be S, as you attempted to send it via SIPR
  - Does NSC / EOP archive content from each PC meeting?
    - What department / who is the POC for this?

don't recall  
what mtg was  
about outside  
email

if package  
was sent  
out

anywhere from  
3 days by  
to right  
before

EMAIL 4  
cont

▪ EMAIL 7 -

- Were there any follow up items?
- What would typically happen after a PC meeting with regards to specific policy / strategy?
- How would decisions from the meeting be disseminated to relevant agencies?

▪ EMAIL 8 & 8a - (header / footer email - tp on way forward in Afghanistan, Plan for PC tomorrow, meeting with Clinton and Petraeus)

- What was the context of this email?
- Do you recall what supporting information was provided by DoS
  - Classification of it?
  - Is it maintained by NSC.

don't recall

- Did you ever have concern about the transmission of sensitive / classified info on unclass, or non-government? → Not that I can recall.
- Any other relevant information?
- NDA

Don't recall ever emailing directly w/ HRC.

PC/DC

1 chair

NSC staffer take notes (responsible for Subj. matter)  
summary of Conclusions / Cleared by NSC executive staff.  
go out through Exec Sec. Wash Fax.

sometimes would call staff of PC or DC to  
tell what agreed to do. - write memo etc.

Sometimes - info gets briefed to President

Wash Fax fairly large distro

- If very sensitive would try to send point to point

- ① get papers
- ② cover note by NSC
- ③ "Read Ahead" - choreography of mtg.

SOC official

rec. of mtg.

goes out to every attendee.  
(not minutes)  
- do ours

HRC-1390

DC Mtg - works on issue - Most focus  
PC Mtg. "  
President - take topic forward -



From: 'Spence, Matthew J.' [redacted]  
Sent: 10/4/2009 11:06:59 PM +00:00  
To: 'Sullivan, Jacob J' <SBUSTATE/SES/RECIPIENTS/SULLIVANJJ>  
Subject: RE: How's it looking?

b6 Per NSC

Thanks man. It's blood out of a stone with the Holbrooke team.

I'm going through the ONI stuff now. It's pretty decent, with a few exceptions.

From: Sullivan, Jacob J (mailto:SullivanJJ@state.gov)  
Sent: Sunday, October 04, 2009 6:34 PM  
To: Spence, Matthew J.  
Subject: Re: How's it looking?

Yes

From: Spence, Matthew J. [redacted]  
To: Sullivan, Jacob J  
Sent: Sun Oct 04 18:29:57 2009  
Subject: RE: How's it looking?

b6 Per NSC

Got it. Another option is for us to courier this stuff out tonight, and then email out your paper very late tonight, since it's at the Secret level, right?

From: Sullivan, Jacob J (mailto:SullivanJJ@state.gov)  
Sent: Sunday, October 04, 2009 6:27 PM  
To: Spence, Matthew J.  
Subject: Re: How's it looking?

Moving as fast as possible.

From: Spence, Matthew J. [redacted]  
To: Sullivan, Jacob J  
Sent: Sun Oct 04 18:20:27 2009  
Subject: How's it looking?

b6 Per NSC

Matt Spence  
National Security Council  
[redacted]

Message Headers:

Internet Headers Version 2.0  
Received: from [redacted] by [redacted] state.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 19:07:15 -0400  
Received: from [redacted] state.sbu [redacted] state.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 19:07:15 -0400  
Received: from [redacted] state.sbu [redacted] state.sbu with I [redacted]  
Sun, 4 Oct 2009 19:07:15 -0400  
Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu w [redacted]  
Sun, 4 Oct 2009 19:07:15 -0400  
Received: from [redacted] by [redacted] state.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 19:07:15 -0400  
Received: from esgeop01.eop.gov (mailhub-esg3.eop.gov [198.137.241.41])  
by stinson2.state.gov with [redacted]  
for <SullivanJJ@state.gov>; Sun, 4 Oct 2009 18:52:33 -0400  
Received: from esgeop01.eop.gov ([198.137.241.41])  
by Stinson-1.state.gov  
for <SullivanJJ@state.gov>; Sun, 04 Oct 2009 23:00:00 -0400  
Received: from esgeop02.eop.gov by esgeop01.eop.gov [redacted] for <SullivanJJ@state.gov>; Sun, 4 Oct 2009 18:52:33 -0400  
X-SENTER-IP: [redacted]  
X-SENTER-REPUTATION: None  
Content-class: urn:content-classes:message  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
[redacted]  
X-MimeOLE: Produced by Microsoft Exchange V6.0.6619.12  
Subject: RE: How's it looking?

b6 Per  
b7E DOS

b6 Per  
b7E DOS

HRC-1392

Date: Sun, 4 Oct 2009 19:06:59 -0400  
Message-ID: <891D44DBD1E2C94EBE988E74EE0C2216013B61C0@SMEOP18EVS.eopds.eop.gov>  
X-MS-Has-Attach:  
X-MS-Exchange-Correlator:  
Thread-Topic: How's it looking?  
Thread-Index: [REDACTED]  
References: [REDACTED] state.sbu>  
From: "Sullivan, Matthew J." [REDACTED]  
To: "Sullivan, Jacob J." <SullivanJJ@state.gov>  
X-OriginalArrivalTime: 04 Oct 2009 23:06:59.0921 (UTC) FILETIME=[REDACTED]  
Return-Path: prvs=52178f90d-[REDACTED]  
X-TM-AS-Product: Ver: [REDACTED]  
X-TM-AS-Result: [REDACTED]  
X-TM-AS-User-Approved-Sender: No  
X-TM-AS-User-Blocked-Sender: No

b6 Per  
b7E DOS

b6 Per NSC

Content-Type: text/plain;  
charset=[REDACTED]  
Content-Transfer-Encoding: base64

Content-Type: text/html;  
charset=[REDACTED]  
Content-Transfer-Encoding: base64

b6 Per  
b7E DOS

PR\_RIM\_INTERNET\_MESSAGE\_ID:  
PR\_RIM\_PAGER\_TX\_FLAG:  
PR\_RIM\_MSG\_FOLDER\_ID:  
PR\_RIM\_DELETED\_BY\_DEVICE:  
PR\_RIM\_MSG\_REF\_ID:  
PR\_RIM\_MSG\_STATUS:  
PR\_RIM\_MSG\_ON\_DEVICE\_3\_5:

<891D44DBD1E2C94EBE988E74EE0C2216013B61C0@SMEOP18EVS.eopds.eop.gov>  
true  
-3  
true  
-2021940588  
1  
true

b6 Per NSC

From: "Spence, Matthew J." [redacted]  
Sent: 10/5/2009 12:46:30 AM +00:00  
To: "Sullivan, Jacob J." <SBUSTATE/SE/RECIPIENTS/SULLIVANJJ>  
Subject: Just sent you the DNI piece on SIPR

Matt Spence

National Security Council

(202) 456-9481

## Message Headers:

Microsoft Mail Internet Headers Version 2.0

Received: from [redacted] slate.sbu [redacted] by [redacted] slate.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 20:46:37 -0400  
Received: from [redacted] slate.sbu [redacted] by [redacted] slate.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 20:46:37 -0400  
Received: from [redacted] slate.sbu [redacted] by [redacted] slate.sbu w [redacted]  
Sun, 4 Oct 2009 20:46:37 -0400  
Received: from slimson2.slate.gov [redacted] by [redacted] slate.sbu with Microsoft [redacted]  
Sun, 4 Oct 2009 20:46:37 -0400  
Received: from esgeop01.eop.gov ([198.137.241.41])  
by slimson2.slate.gov with [redacted]  
for <SullivanJJ@slate.gov>; Sun, 4 Oct 2009 20:32:04 -0400  
Received: from esgeop01.eop.gov ([198.137.241.41])  
by Slimson-1.slate.gov  
for <SullivanJJ@slate.gov>; Mon, 05 Oct 2009 00:53:46 +0000  
Received: from esgeop02.eop.gov by esgeop01.eop.gov [redacted] for <SullivanJJ@slate.gov>; Sun, 4 Oct  
X-SENDER-IP: [redacted]  
X-SENDER-REPUTATION: None  
Content-Class: urn:content-classes:message  
MIME-Version: 1.0  
Content-Type: multipart/alternative;

X-MimeDLE: Produced By Microsoft Exchange [redacted]  
Subject: Just sent you the DNI piece on SIPR  
Date: Sun, 4 Oct 2009 20:46:30 -0400  
Message-ID: <891D44DBD1E2C94EBE988E74EE0C2216013B61CF@SMEDP18EVS.eopds.eop.gov>  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
Thread-Topic: Just sent you the DNI piece on SIPR  
Thread-Index: [redacted]  
From: "Spence, Matthew J." [redacted]  
To: "Sullivan, Jacob J." <SullivanJJ@slate.gov>  
X-OriginalArrivalTime: 05 Oct 2009 00:46:30.0953 (UTC) FILETIME=[redacted]  
Return-Path: prvs=S22d21f15-[redacted]  
X-TM-AS-Product-Version: [redacted]  
X-TM-AS-Result: [redacted]  
X-TM-AS-User-Approved-Sender: No  
X-TM-AS-User-Blocked-Sender: No

[redacted]  
Content-Type: text/plain;  
charset=[redacted]  
Content-Transfer-Encoding: quoted-printable

[redacted]  
Content-Type: text/html;  
charset=[redacted]  
Content-Transfer-Encoding: quoted-printable

PR\_RIM\_INTERNET\_MESSAGE\_ID: <891D44DBD1E2C94EBE988E74EE0C2216013B61CF@SMEDP18EVS.eopds.eop.gov>  
PR\_RIM\_PAGER\_TX\_FLAG: Invo  
PR\_RIM\_MSG\_FDLOER\_ID: -3  
PR\_RIM\_DELETED\_BY\_DEVICE: Invo  
PR\_RIM\_MSG\_REF\_ID: -1375815399  
PR\_RIM\_MSG\_STATUS: 1  
PR\_RIM\_MSG\_DN\_DEVICE\_3\_5: Invo

b6 Per  
b7E DOSb6 Per  
b7E DOS

b6 Per NSC

HRC-1394

From: "Spence, Matthew J." [redacted]  
Sent: 10/5/2009 11:35:36 AM +00:00  
To: "Sullivan, Jacob J" <SBUSTATE/SES/RECIPIENTS/SULLIVANJJ>  
Subject: State paper

b6 Per NSC

Hey man -

Sorry to sound like a broken record, but know when you all could shoot that paper over?

I also saw that the DNI thing I sent on SIPR didn't go through for some reason. But the package was couriered over, so you all should have it by now.

Matt Spence

National Security Council

(202) 456-9481

## Message Headers:

Microsoft Mail Internet Headers Version 2.0  
Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with Microsoft [redacted]  
Mon, 5 Oct 2009 07:35:44 -0400  
Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with Microsoft [redacted]  
Mon, 5 Oct 2009 07:35:44 -0400  
Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with I [redacted]  
Mon, 5 Oct 2009 07:35:44 -0400  
Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu w [redacted]  
Mon, 5 Oct 2009 07:35:44 -0400  
Received: from slimson3.state.gov [redacted] by [redacted] state.sbu with Microsoft [redacted]  
Mon, 5 Oct 2009 07:35:43 -0400  
Received: from esgeop01.eop.gov ([198.137.241.41])  
by slimson3.state.gov with [redacted]  
for <SullivanJJ@state.gov>; Mon, 5 Oct 2009 07:29:48 -0400  
Received: from esgeop01.eop.gov ([198.137.241.41])  
by Slimson-2.state.gov  
for <SullivanJJ@state.gov>; Mon, 05 Oct 2009 11:45:18 +0000  
Received: from esgeop02.eop.gov by esgeop01.eop.gov [redacted] for <SullivanJJ@state.gov>; Mon, 5 Oct  
X-SENDER-IP: [redacted]  
X-SENDER-REPUTATION: None  
Content-Class: urn:content-classes:message  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
[redacted]  
X-MimeOLE: Produced By Microsoft Exchange [redacted]  
Subject: State paper  
Date: Mon, 5 Oct 2009 07:35:36 -0400  
Message-ID: <8910440BD1E2C94E8E988E74EE0C2216013B61D8@SMEOP18EVS.eopds.eop.gov>  
X-MS-Has-Attach:  
X-MS-TNEF-Correlator:  
Thread-Topic: State paper  
Thread-Index: [redacted]  
From: "Spence, Matthew J." [redacted]  
To: "Sullivan, Jacob J" <SullivanJJ@state.gov>  
X-OriginalArrivalTime: 05 Oct 2009 11:35:36.0974 (UTC) FILETIME=[redacted]  
Return-Path: prvs=522d21f15 [redacted]  
X-TM-AS-Product-Version: [redacted]  
X-TM-AS-Result: No [redacted]  
X-TM-AS-User-Approved-Sender: No  
X-TM-AS-User-Blocked-Sender: No

b6 Per  
b7E DOSb6 Per  
b7E DOS

b6 Per NSC

b6 Per  
b7E DOS

PR\_RIM\_INTERNET\_MESSAGE\_ID:  
PR\_RIM\_PAGER\_TX\_FLAG:  
PR\_RIM\_MSG\_FOLDER\_ID:  
PR\_RIM\_DELETED\_BY\_DEVICE:  
PR\_RIM\_MSG\_REF\_ID:  
PR\_RIM\_MSG\_STATUS:  
PR\_RIM\_MSG\_ON\_DEVICE\_3\_6:

[redacted]  
<8910440BD1E2C94E8E988E74EE0C2216013B61D8@SMEOP18EVS.eopds.eop.gov>  
true  
-3  
true  
-1660938066  
1  
true

From: "Spence, Matthew J." [redacted]  
Sent: 10/4/2009 11:53:27 PM +00:00  
To: "Sullivan, Jacob J" <SBUSTATE/SES/RECIPIENTS/SULLIVANJJ>  
Subject: RE: How's it looking?

b6 Per NSC

Getcha,

I'm gonna send this out now, but you'd help your cause a lot with Tom if you could have something that he can read when he walks in tomorrow morning (which I could read first).

The DNI stuff is actually pretty lame and doesn't help. But it's secret, so I'll send it to you on SIPR.

From: Sullivan, Jacob J (mailto:SullivanJJ@state.gov)  
Sent: Sunday, October 04, 2009 7:37 PM  
To: Spence, Matthew J.  
Subject: RE: How's it looking?

This is tough, but part of it is S engagement. She wants to see final and edit before it goes.

From: Spence, Matthew J. (mailto:[redacted])  
Sent: Sunday, October 04, 2009 7:07 PM  
To: Sullivan, Jacob J  
Subject: RE: How's it looking?

b6 Per NSC

Thanks man, it's blood out of a stone with the Holbrooke team.

I'm going through the DNI stuff now. It's pretty decent, with a few exceptions.

From: Sullivan, Jacob J (mailto:SullivanJJ@state.gov)  
Sent: Sunday, October 04, 2009 6:34 PM  
To: Spence, Matthew J.  
Subject: Re: How's it looking?

Yes

From: Spence, Matthew J. [redacted]  
To: Sullivan, Jacob J  
Sent: Sun Oct 04 18:29:57 2009  
Subject: RE: How's it looking?

b6 Per NSC

Getcha, Another option is for us to courier this stuff out tonight, and then email out your paper very late tonight, since it's at the secret level, right?

From: Sullivan, Jacob J (mailto:SullivanJJ@state.gov)  
Sent: Sunday, October 04, 2009 6:27 PM  
To: Spence, Matthew J.  
Subject: Re: How's it looking?

Moving as fast as possible.

From: Spence, Matthew J. [redacted]  
To: Sullivan, Jacob J  
Sent: Sun Oct 04 18:20:27 2009  
Subject: How's it looking?

b6 Per NSC

Matt Spence

HRC-1396

From: "Spence, Matthew J." [redacted]  
 Sent: 10/4/2009 11:06:30 PM +00:00  
 To: "Jones, Paul W." <SBUSTATE/MANILA AG/RECIPIENTS/JONESPW2>; "Sullivan, Jacob J." <SBUSTATE/SES/RECIPIENTS/SULLIVANJJ>  
 CC: "Tien, John K." [redacted]; "Lebson, Eric M." [redacted]  
 Subject: RE: How's it looking?

b6 Per NSC

The folks here have asked you to send it here, and we'll do the disiro with the package. It'll come on SIPR? Can you send a draft here, which we won't disiro beyond the few folks working on it here?

Looping in our folks handling this.

From: Jones, Paul W. [mailto:JonesPW2@state.gov]  
 Sent: Sunday, October 04, 2009 6:45 PM  
 To: Sullivan, Jacob J.; Spence, Matthew J.  
 Subject: RE: How's it looking?

It is not ready for disiro - still a number of items. I think we need to email late tonight. Just let me know the address(es).

John,

We can provide a draft now for S, if needed.

From: Sullivan, Jacob J.  
 Sent: Sunday, October 04, 2009 6:36 PM  
 To: [redacted] Jones, Paul W.  
 Subject: Re: How's it looking?

b6 Per NSC

Adding Paul, Paul what's our ETA?

From: Spence, Matthew J. [redacted]  
 To: Sullivan, Jacob J.  
 Sent: Sun Oct 04 18:29:57 2009  
 Subject: RE: How's it looking?

Gotcha. Another option is for us to courier this stuff out tonight, and then email out your paper very late tonight, since it's at the Secret level, right?

From: Sullivan, Jacob J. [mailto:SullivanJJ@state.gov]  
 Sent: Sunday, October 04, 2009 6:27 PM  
 To: Spence, Matthew J.  
 Subject: Re: How's it looking?

Moving as fast as possible.

From: Spence, Matthew J. [redacted]  
 To: Sullivan, Jacob J.  
 Sent: Sun Oct 04 18:20:27 2009  
 Subject: How's it looking?

b6 Per NSC

Max Spence

National Security Council

b6 Per  
 b7E DOS

Message Headers:

Microsoft Mail Internet Headers Version 2.0  
 Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with Microsoft [redacted]  
 Sun, 4 Oct 2009 19:06:37 -0400  
 Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with Microsoft [redacted]  
 Sun, 4 Oct 2009 19:06:37 -0400  
 Received: from [redacted] state.sbu [redacted] by [redacted] state.sbu with Micro  
 Sun, 4 Oct 2009 19:06:37 -0400

HRC-1397

From: "Spence, Matthew J." [REDACTED]  
 Sent: 10/5/2009 9:44:10 PM +0000  
 To: "Sullivan, Jacob J" <JSULLIVAN@STATE.SES/RECIPIENTS/SULLIVANJJ>  
 Subject: Checking in

b6 Per NSC

Hey man - Let me sort out the follow-ups from this mtg, then give you a call to check in on all of this...

Matt Spence

National Security Council

Message Headers:

Microsoft Mail Internet Headers Version 2.0  
 Received: from [REDACTED]@state.sbu [REDACTED] by [REDACTED]@state.sbu with Microsoft Exchange [REDACTED] Mon, 5 Oct 2009 17:44:28 -0400  
 Received: from [REDACTED]@state.sbu [REDACTED] by [REDACTED]@state.sbu with Microsoft Exchange [REDACTED] Mon, 5 Oct 2009 17:44:28 -0400  
 Received: from [REDACTED]@state.sbu [REDACTED] by [REDACTED]@state.sbu with Microsoft Exchange [REDACTED] Mon, 5 Oct 2009 17:44:27 -0400  
 Received: from slimson3.state.gov [REDACTED] by [REDACTED]@state.sbu with Microsoft Exchange [REDACTED] Mon, 5 Oct 2009 17:44:27 -0400  
 Received: from esgeop01.eop.gov ([198.137.241.41]) [REDACTED] by slimson3.state.gov with Microsoft Exchange [REDACTED] for <SullivanJ@state.gov>; Mon, 5 Oct 2009 17:38:32 -0400  
 Received: from esgeop01.eop.gov ([198.137.241.41]) [REDACTED] by Slimson-2.state.gov with Microsoft Exchange [REDACTED] for <SullivanJ@state.gov>; Mon, 05 Oct 2009 21:54:07 +0000  
 Received: from esgeop02.eop.gov by esgeop01.eop.gov id 19813724141 for <SullivanJ@state.gov>; Mon, 5 Oct 2009 17:44:10 -0400  
 X-SENDER-IP: [REDACTED]  
 X-SENDER-REPUTATION: None  
 Content-Class: urn:content-classes:message  
 MIME-Version: 1.0  
 Content-Type: text/plain; charset=utf-8; alternative=[REDACTED]  
 X-MimeOLE: Produced by Microsoft Exchange [REDACTED]  
 Subject: Checking in  
 Date: Mon, 5 Oct 2009 17:44:10 -0400  
 Message-ID: <891D440BD1E2C94EBE988E74EE0C2216013B61EE@SMEOP18EVS.eopds.eop.gov>  
 X-MS-Exchange-Organization: [REDACTED]  
 X-MS-Exchange-Correlation: [REDACTED]  
 Thread-Topic: Checking in  
 Thread-Index: [REDACTED]  
 From: "Spence, Matthew J." [REDACTED]  
 To: "Sullivan, Jacob J" <SullivanJ@state.gov>  
 X-OriginalArrivalTime: 05 Oct 2009 21:44:10.0403 (UTC) FILETIME=[REDACTED]  
 Return-Path: prvs=522d21115-[REDACTED]  
 X-TM-AS-Product-Version: [REDACTED]  
 X-TM-AS-Result: [REDACTED]  
 X-TM-AS-User-Approved-Sender: No  
 X-TM-AS-User-Blocked-Sender: No

b6 Per

b7E DOS

b6 Per

b7E DOS

b6 Per

b7E DOS

b6 Per NSC

Content-Type: text/plain;  
 charset=[REDACTED]  
 Content-Transfer-Encoding: quoted-printable

Content-Type: text/html;  
 charset=[REDACTED]  
 Content-Transfer-Encoding: quoted-printable

b6 Per

b7E DOS

PR\_RIM\_INTERNET\_MESSAGE\_ID:  
 PR\_RIM\_PAGER\_TX\_FLAG:  
 PR\_RIM\_MSG\_FOLDER\_ID:  
 PR\_RIM\_DELETED\_BY\_DEVICE:  
 PR\_RIM\_MSG\_REF\_ID:  
 PR\_RIM\_MSG\_STATUS:  
 PR\_RIM\_MSG\_ON\_DEVICE\_3\_6:

<891D440BD1E2C94EBE988E74EE0C2216013B61EE@SMEOP18EVS.eopds.eop.gov>  
 true  
 -3  
 true  
 -1882870175  
 1  
 true

om: "McClure, Kimberly M" <SBUSTATE/SES/RECIPIENTS/MCCLUREKM>  
nt: 10/5/2009 12:20:00 PM +00:00  
: "Jones, Paul W" <JonesPW2@state.gov>; "Sullivan, Jacob J"  
<SullivanJJ@state.gov>  
>: SSRAP\_StaffAssistants <SSRAP\_StaffAssistants@state.gov>  
bjeet: RE: Materials for wh

e just talked to Matt Spence. We're having it washfaxed now.

--Original Message-----

om: Jones, Paul W  
nt: Monday, October 05, 2009 7:05 AM  
: Sullivan, Jacob J; McClure, Kimberly M  
bjeet: RE: Materials for wh

e-emailed and Kim will follow up to ensure they received. If not, we will washfax.

--Original Message-----

om: Sullivan, Jacob J  
nt: Monday, October 05, 2009 8:04 AM  
: Jones, Paul W; LaVine, Christopher M; Beale, Courtney A Kramer  
bjeet: Materials for wh

hite House is having email probs so can you guys washfax and re-email to wh folks?

R\_RIM\_INT: \_MESS

SE\_ID: state.sbu>

R\_RIM\_PAGER\_TX\_FLAG: true

R\_RIM\_MSG\_FOLDER\_ID: -3

R\_RIM\_DELETED\_BY\_DE

CE:

R\_RIM\_MESSAGE\_SUBMI

SION\_ID:

R\_RIM\_MSG\_REF\_ID: -1837087385

R\_RIM\_MSG\_STATUS: 1

R\_RIM\_MSG\_ON\_DEVICE true

\_6:

b6 Per  
b7E DOS

b6 Per  
b7E DOS



**From:** "Toiv, Nora F" <CLASSIFIED/SES AC/RECIPIENTS/TOIVNF>  
**Sent:** 10/5/2009 12:35:25 PM -0000  
**To:** "Mills, Cheryl D" <MillsCD@state.gov>  
**Subject:** FW: FW: Final Pak Memo w/ attachments  
**Attachments:** Tab 7 - Proposed Signature Assistance Program.ppt; Tab 1 - Riedel Objectives.docx; Tab 3 - Pakistan's Support for Taliban and Terrorism - FINAL.docx; Tab 4 - Security Assistance Proposal.ppt; Tab 5 - Stabilizing Pakistan.docx; Tab 6 - Current US Civilian Assistance.docx; Tab 8 - PakistanStrategy Abbreviated version.ppt; Tab 10 - Alternative Approaches.docx; Tab 9 - Intl Support for Pakistan.docx; MLC - US Interests in Pak Paper 10-04.pdf; 09-10-5 SEC-JONES MEMO on Pak.pdf

**From:** Beale, Courtney A  
**Sent:** Monday, October 05, 2009 8:31 AM  
**To:** Toiv, Nora F; Laszczych, Joanne  
**Cc:** 5\_SpecialAssistants  
**Subject:** FW: Final Pak Memo w/ attachments  
**Importance:** High

**From:** McClure, Kimberly M **On Behalf Of** SSRAP Staff Assistants  
**Sent:** Monday, October 05, 2009 8:18 AM  
**To:** 5\_SpecialAssistants  
**Cc:** SSRAP\_StaffAssistants  
**Subject:** FW: Final Pak Memo w/ attachments  
**Importance:** High

Courtney, Zia, Dan -

I just wanted to make sure a copy of this had made its way to you as well. This is for today's restricted PC on Af-Pak.

Kim McClure

Special Assistant

Office of the Special Representative for Afghanistan and Pakistan

HRC-1400

202-647-4134

**From:** McClure, Kimberly M **On Behalf Of** SSRAP Staff Assistants  
**Sent:** Monday, October 05, 2009 8:15 AM  
**To:** Dubose, Mary L  
**Cc:** D(L); SSRAP\_Staff Assistants  
**Subject:** FW: Final Pak Memo w/ attachments  
**Importance:** High

Mary,

Here is the package for today's NSC meeting (there is no Tab 2, as it is a TS doc that will be provided by ODNI). Please note that an Annotated Agenda was submitted to the Line on Friday. They will have the latest version of that document.

Kim McClure

Special Assistant

Office of the Special Representative for Afghanistan and Pakistan

202-647-4134

**From:** Jones, Paul W  
**Sent:** Monday, October 05, 2009 4:09 AM  
**To:** Spence, Matthew; Sullivan, Jacob J; 'Kobs, David M.'; 'Tien, John K. Jr.'; 'Lute, Douglas E.'; Lebson, Eric  
CIV OSD POLICY; Chollet, Derek H  
**Cc:** SSRAP\_Staff Assistants  
**Subject:** FW: Final Pak Memo w/ attachments  
**Importance:** High

Dear NSC colleagues,

Pls find attached a cover memo from Secretary Clinton, the State Dept memo U.S. interests in Pakistan, and ten tabs, for the Principals meeting on Tuesday afternoon. We would appreciate your circulating these materials to attendees at the Principals committee meeting.

Note 2- Tab 2 to be provided by ODNI.

Best regards,

HRC-1401

Paul

---



RELEASE IN PART B5,B6

---

**From:** Sullivan, Jacob J <SullivanJJ@state.gov>  
**Sent:** Friday, June 17, 2011 8:18 AM  
**To:** H  
**Subject:** Re: [REDACTED]

B5

They say they've had issues sending secure fax. They're working on it.

---

**From:** Sullivan, Jacob J  
**Sent:** Friday, June 17, 2011 08:00 AM  
**To:** 'HDR22@clintonemail.com' <HDR22@clintonemail.com>  
**Subject:** Re: [REDACTED]

?!!! Checking

---

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Friday, June 17, 2011 07:52 AM  
**To:** Sullivan, Jacob J  
**Subject:** Re: [REDACTED]

I didn't get the TPs yet.

---

**From:** Sullivan, Jacob J [mailto:SullivanJJ@state.gov]  
**Sent:** Thursday, June 16, 2011 05:51 PM  
**To:** H  
**Subject:** Fw: [REDACTED]

You'll get tps this eve. They're coming together.

---

**From:** Spence, Matthew J. [mailto:[REDACTED]]  
**Sent:** Thursday, June 16, 2011 04:15 PM  
**To:** Sullivan, Jacob J  
**Subject:** [REDACTED]

B6

B5

[REDACTED]

1A49

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

56

Date Received

2-18-2016

From

[Redacted]

(Name of Contributor/Interviewee)

b6  
b7C

(Address)

Washington DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Midyear Exam

Reference:

Notes from

[Redacted]

Interview

(Communication Enclosing Material)

b6  
b7C

Description:

☒

Original notes re interview of

[Redacted]

b6  
b7C

1A49

HRC-1404

~~SECRET~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-21-2016 BY J76J18T80 NSICG

2/18/2016

[REDACTED]

b6  
b7C

- Current info from 2013.

[REDACTED]

b6  
b7C

- TEAM MEMBERS HAD ACCESS TO intel

[REDACTED]

b6  
b7C

[REDACTED]

- Regular interaction w/ DOS

b1 Per  
b3 CIA

@ [REDACTED] → DOS close relationship [REDACTED] (S)

close coordination and all [REDACTED] of DOS

Entity,

- [REDACTED] EHC had prior relation & close working

b6  
b7C

- interacted weekly on average

@ [REDACTED] → more frequent interaction w/ DOS

[REDACTED] / EHC [REDACTED]

had weekly lunch, coordinated on  
everything "down range"

known  
since [REDACTED]

Sec's SE TEAM / FEINT OFFICE

Primary contacts = MILLS, SULLIVAN, [REDACTED]  
sometimes w/ AMBASSADORS.

OFFICE

b6  
b7C

- "my boss & your boss should talk about"

~~SECRET~~

HRC-1405

How did you com?

- PHONE AND EMAIL Connectivity.

- "intersecting TRAVE"

- EMAIL / PHONE, less FREQ MEETINGS.

° USED CLASSIFIED EMAIL SYSTEMS AT  
BOOTH AGENCIES.

→ PRIMARY ON UNCLASS SYSTEM

HAD SIPR & JOWICS.

→ SPOOF TYPE STUFF → more sensitive.

→ MAIN PHONE WAS "open line"

RED PHONE (yellow) was secure

→ MAY HAVE HAD A BACKUP.

- with phone (classified) → internal

→ external, COORDINATION.

BACK (UNCLASSIFIED)

- DEFAULT IS High SIDE

- Agency Information Network (low side)

→ STE AT HOME, AND A SAFE

TRANSFER TO DOS.

- DOESN'T RECALL PHYSICAL TRANSFER TO DOS.

- EMAIL ON BOOTH High & Low SIDE

↳ NO DIRECT EMAILS w/ HC

→ NO KNOWLEDGE OF Server / EMAIL

- HAD DIRECT CONTACT w/ HC

mostly in person  
MAYBE PHONE BUT RELIED  
ON TEAMS

NSC MEETINGS

~~SECRET~~

HRC-1406

~~SECRET~~

MESSAGES FROM [ ] TO HC. CONSIDERED  
BY [ ] WOULD PASS TO HC SR STAFF  
AS APPROPRIATE.

b6  
b7C

EMAIL 1 [ ]

b3 Per CIA  
b6 Per FBI  
b7C Per FBI

- FEW WEEKS AFTER [ ] STARTS POSITION.  
- SLIGHT RECOLLECTION

- NOT "OFFICIAL DOWNLOAD" THAT WOULD BE  
[ ] <sup>1 -> NY BRUSE</sup>  
THIS WAS AN INTERESTING  
EXCHANGE / SIDENOTE

b3 Per CIA

EMAIL 2 [ ]

b3 Per CIA  
b6 Per FBI, CIA  
b7C Per FBI

[ ] (SOME OF THIS [ ]  
[ ] CALLED BY EA W/ OFFICE. CONTACTED [ ]  
[ ] ASKED THEM TO CONTACT [ ] (w/ HI),  
VP, CHAIRMAN of Joint Chiefs, Sec State, Sec Def.  
- DON'T RECALL SPECIFIC CALL FROM [ ]  
MAY HAVE BEEN VIA STE  
- DOESN'T RECALL CALL w/ [ ] BUT MOST  
CALLS THAT DAY WERE <sup>MOST LIKELY</sup> ON UNCLASS LINE  
(DUE TO EMERGENCY OF THE SITUATION).  
- MAY HAVE BEEN FOLLOW UP CALLS ON THE STE, ETC  
- THIS IS A "GIVE YOUR BOSS A HEADS UP THE MESSAGE"

b6  
b7C

HRC-1407

~~SECRET~~





~~SECRET~~

SMAL G- GREEN ON BLUE (REDACTED VERIFIED)

• RAPID COORDINATION ESTABL [REDACTED] & DoS

b6  
b7C

PUBLIC AFFAIRS RE: TERRORIST ATTACK

" [REDACTED] WAS DoS PR POC

b6  
b7C

[REDACTED] WAS [REDACTED] PR POC

le:  
Needs  
[REDACTED]

→ [REDACTED]

b6  
b7C

→ DIDN'T SAY [REDACTED]

b1 Per CIA  
(S) b6 Per FBI  
b7C Per FBI

I DON'T KNOW IF IT IS TRUE

(S) [REDACTED]

- NO CONCERNS [REDACTED] DoS  
HANDLING OF [REDACTED] INFO

~~SECRET~~

HRC-1409

~~SECRET~~

b6  
b7C

[redacted] Interview Outline

b6  
b7C

Professional Background

- Founder and Managing Director [redacted] (2013 – Present; founded [redacted])
- [redacted]
- Various roles on [redacted]

Intel Matters until [redacted]

Educational Background

- [redacted]
- [redacted]

b6  
b7C

Question Outline

- Introduction
  - FBI's interest in the matter
  - NSLB disclaimer re: prior statements
  - Can consult counsel if necessary
- What is your current position?
- Brief description of role as [redacted] relative to Department of State?

More frequent

down range coordination

b1 Per CIA  
b3 Per CIA  
b6 Per FBI  
b7C Per FBI

Close Relationship

(S) very close coordination all levels all the time weekly.

Default Email @ [redacted] on High Side - used more rarely  
worked for wte. knew Clinton for 20+ years

- How often did you coordinate with DoS?
  - For what type of matters?
  - Who were your primary contacts at DoS while at [redacted]?
  - What was the nature of the communications? (in person, email, telephone)
  - How often did you send / receive documents to DoS?
    - Examples of?
      - Classified, unclassified?
      - How were the documents transferred?

Milk Sullivan

Amb. occasionally

- Did you ever email directly with Secretary Clinton?
- Were you aware of Secretary Clinton's use of a private email address? Private server?
- Did [redacted] ever acknowledge to you he was aware Secretary Clinton was using a private/non DoS email account?

b6  
b7C

START of emails during [redacted] Tenure... If [redacted] wanted to contact HRC direct how was this done?

b3 Per CIA  
b6 Per FBI  
b7C Per FBI

- Email #1: [redacted] (March 21, 2009)

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted] forward to HRC from his personal email [redacted] is this the account to which you would have sent?

Unclass came up. Mostly work on SIPR - general FP. JWCIS... TS or more intel.

- Was it common practice to send [redacted] this kind of information?

official download went to WH. poss NAT Sec. Advisor.

Main line open line Yellow but called Red.

weekly lunch w/ [redacted]

DoS Sec. HRC-1410

NSA Chairman

~~SECRET~~

~~SECRET~~

call

COJC  
Sec Det  
Sec State

How did you receive info.

@home in Carmel Valley.  
Pres. Hawaii's VP on travel.

- Email #2: [redacted] (December 30, 2009) from [redacted] to Secretary Clinton referencing call with [redacted]

b6  
b7C

- Do you recall how the call referenced in the email with [redacted] was conducted? (secure/unsecure) Assume "open line" means unclass?

Initial call from

- Reason for call being on an open line?

EA [redacted]

- Reference "details are thin and couldn't get into more detail on an open line..."

Where/How do you draw the line between what can be discussed on an open line vs. b3 Per CIA move to a classified venue?

- Were you aware or did you assume [redacted] would forward the information on to the Secretary?

- Were you aware he would email the information? Unclass? From Gmail Account?

b3 Per CIA  
b6 Per CIA, FBI  
b7C Per FBI

- Email #3: [redacted] Email" (January 10, 2010)

- [redacted] - was this the unclassified account you primarily used for work purposes?

- [redacted] (until [redacted]) - work email not available.

- [redacted] (starting on [redacted]) - BB w/ unclass [redacted] email

- Email #4: [redacted] n Israel" (November 20, 2010)

b3 Per CIA  
b6 Per FBI  
b7C Per FBI

- This was sent from Gmail to Sullivan via Gmail...

- Can you recall why you emailed via Gmail at the time?
- Common practice in regards to Sullivan? Instructions to do so for this instance?
- Why would you email Sullivan via Gmail vs. DoS account?

START of emails related to [redacted] TENURE...

b6  
b7C

- Email #5: [redacted] (Dated September 11, 2012) - B5 Redaction

- So [redacted] the information a conversation between [redacted] and the Joint Staff?

Consultation

- Any official documentation of conversation?
- Classification of material?

b6  
b7C

- Email #6: "This am Green on Blue" (October 13, 2012) - B1 Redaction

b1 Per CIA  
b6 Per FBI  
b7C Per FBI

- Explain email?

- Recipients? Why [redacted] and [redacted] (S)

- Reference to [redacted] and [redacted]

- [redacted]

- Confirm [redacted] quote
- To whom?
- Circumstances?

Rapid Coordination

DoS. Public Affairs [redacted]

b6  
b7C

Sent [redacted] Email w/ view "jacked up"

HRC-1411

~~SECRET~~

~~SECRET~~

- Did you ever have concern regarding the transmission of sensitive / classified info on unclass, or non-government, systems?
- Any other relevant information?
- NDA

~~SECRET~~

HRC-1412

**From:** [REDACTED]  
**Sent:** Saturday, March 21, 2009 2:58 PM  
**To:** H  
**Cc:** Huma Abedin  
**Subject:** [REDACTED]

b3 Per DOS, CIA

I think you know that my close friend Jeremy Bash is now Panetta's Chief of Staff at CIA. [REDACTED]  
[REDACTED]  
[REDACTED]

###

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 30, 2009 12:52 PM  
**To:** H  
**Cc:** CDM; Huma Abedin; Jake Sullivan  
**Subject:** CIA

b6 Per  
b7C DOS

Separate from what's happening in regards to the Christmas attack, Jeremy Bash just called me because Director Panetta wanted him to relay through me that the CIA suffered a terrible incident yesterday in Afghanistan.

Seven of their agents were meeting with a contact when an explosion killed them all. To the extent it's currently being reported, they are being identified as DoD personnel, not Agency.

The details are thin and he couldn't get into more detail on an open line, but they believe the contact they met with was them up and was either carrying the explosive or detonated it.

They believe this is the greatest loss of life to a single incident in the Agency's history, and the first time that Agency personnel have been so deliberately targeted in Afghanistan.

Director Panetta's at home in Monterey, CA, and likely returning to DC in the coming days.

**From:** [REDACTED]

b6 Per  
b7C DOS

**Sent:** 2/10/2010 12:17:53 AM +00:00

**To:** "Sullivan, Jacob J" <SullivanJJ@state.gov>

**Subject:** [REDACTED] Bash email

That's what he uses

---

**From:** Sullivan, Jacob J

**To:** [REDACTED]

**Sent:** Tue Feb 09 19:16:28 2010

**Subject:** Re: Bash email

b6 Per  
b7C DOS

Work email?

---

**From:** [REDACTED]

**To:** Sullivan, Jacob J

**Cc:** [REDACTED]

**Sent:** Tue Feb 09 18:31:51 2010

**Subject:** Re: Bash email

b6 Per DOS, CIA  
b7C Per DOS

---

**From:** Sullivan, Jacob J

**To:** [REDACTED]

**Sent:** Tue Feb 09 18:30:13 2010

**Subject:** Bash email

b6 Per  
b7C DOS

Can you send me Jeremy's email?

-----  
**Message Headers:**

Microsoft Mail Internet Headers Version 2.0

Received: from [REDACTED] state.sbu ([REDACTED])

Tue, 9 Feb 2010 19:17:53 -0500

Received: from [REDACTED] state.sbu ([REDACTED])

Tue, 9 Feb 2010 19:17:53 -0500

Received: from [REDACTED] state.sbu ([REDACTED])

Microsoft [REDACTED]

Tue, 9 Feb 2010 19:17:52 -0500

b6 Per  
b7E DOS

HRC-1415



15-LR-0002

---

**From:** Bash, Jeremy CIV SD [REDACTED] (b)(6)  
**Sent:** Tuesday, September 11, 2015 PM  
**To:** Sullivan, Jacob J; Shanahan, William R; Nides, Thomas R  
**Cc:** Miller, James HON OSD POLICY; Winnefeld, James A ADM JCS VCJCS; Kelly, John LtGen  
**Subject:** SD; martin.dempsey (b)(6)  
Libya

State colleagues:

I just tried you on the phone but you were all in with S.

After consulting with General Dempsey, General Ham and the Joint Staff, we have identified the forces that could move to Benghazi. They are spinning up as we speak. They include a [REDACTED] (b)(5)

[REDACTED] (b)(5)

Assuming Principals agree to deploy these elements, we will ask State to secure the approval from host nation. Please advise how you wish to convey that approval to us. [REDACTED] (b)(5)

[REDACTED] (b)(5)

Jeremy

RELEASE IN PART  
B1,1.4(D),1.4(C),B6

**From:** Mills, Cheryl D <MillsCD@state.gov>  
**Sent:** Saturday, October 13, 2012 10:11 AM  
**To:** H  
**Subject:** Fw: This am Green on Blue

Classified by DAS, A/GIS, DoS on 01/29/2016 ~  
Class: SECRET ~ Reason: 1.4(C), 1.4(D) ~ Declassify  
on: 10/12/2027

----- Original Message -----

**From:** Reines, Philippe I  
**Sent:** Saturday, October 13, 2012 09:53 AM  
**To:** Mills, Cheryl D; Sullivan, Jacob J  
**Subject:** Fw: This am Green on Blue

----- Original Message -----

**From:** Bash, Jeremy CIV SD (mailto:[redacted])  
**Sent:** Saturday, October 13, 2012 09:45 AM  
**To:** Little, George CIV OSD PA <[redacted]>; Reines, Philippe I  
**Cc:** Kelly, John LtGen SD <[redacted]>; Waldhauser, Thomas LtGen SD <[redacted]>  
**Subject:** This am Green on Blue

B6

As you'll be hearing from ISAF, an Afghan NDS officer pulled the ripcord on a vest in front of coalition guys loading a helicopter. Total of 14 either killed or wounded -- some US, some Afghans.

Right now, we think 1 US mil killed and one wounded.

[redacted]

1.4(C)  
1.4(D)  
B1

George, please lash up with [redacted]

B6

HRC-1418

NEWS FEB 4 2016, 5:00 AM ET

## Clinton Emails Held Indirect References to Undercover CIA Officers

by KEN DILANIAN

A handful of emails forwarded to Hillary Clinton's personal server while she was secretary of state contained references to undercover CIA officers — including one who was killed by a suicide attack in Afghanistan, according to U.S. officials who have reviewed them.

But contrary to some published reports, three officials said there was no email on Clinton's server that directly revealed the identity of an undercover intelligence operative. Rather, they said, State Department and other officials attempted to make veiled references to intelligence officers in the emails — references that were deemed classified when the messages were being reviewed years later for public release.



Hillary Clinton takes a question at a rally in New Hampshire on Feb. 3, 2016. ADREES LATIF / Reuters

In one case, an official said, an undercover CIA officer was referred to as a State Department official with the word "State," in quotes, as if to suggest the emailer knew the officer was not actually a diplomat. In another case, an email refers to "OGA" for "other government agency," a common reference to the CIA. Yet another now-classified email chain originated with a member of the CIA director's staff, leading some officials to question how Clinton could be blamed.

**Related: Judge Sets Hearing Date in Clinton Email Case**

Clinton campaign spokesman Brian Fallon said no intelligence officer had been identified in the emails, and that misleading details from the emails were being leaked to hurt the candidate.

"This shows yet again how the leaking of selective details gives a completely false impression about what is actually contained in the emails forwarded to Hillary Clinton," said Fallon. "Whenever the full contents of these emails are learned, there is invariably less than meets the eye."

Twenty-two of the emails were fully withheld from public release last week on the grounds that the information in them is "Top Secret," meaning its disclosure now would cause "exceptionally grave damage to the national security." But intelligence officials and congressional officials who oversee them are divided over whether that is actually the case.

Nonetheless, the issue promises to dog Clinton's presidential campaign. Since the messages are classified, people with the clearances to see them are free to characterize them as they wish. Republicans tend to see them as highly problematic for Clinton, while Democrats see the opposite. The FBI is investigating the security of Clinton's email arrangement, and the FBI would also have jurisdiction to investigate the mishandling of classified information.

Sen. Marco Rubio, the Florida Republican running for president, serves on the Senate Intelligence Committee. "If someone on my staff did what she did...they would be fired and they would be prosecuted," he said recently.

But Rep. Adam Schiff of California, a Clinton supporter who is the ranking Democrat on the House Intelligence Committee, offered a different view after reading the emails.

"The determination that something is top secret, for many people connotes that these are the most closely held secrets, that their revelation would be extremely damaging," he said. "There are potentially programs that are talked about all the time in the press that fit within that category."

Schiff may have been referring to CIA drone strikes, which officials have said are discussed in the now-classified emails. The strikes are highly classified but are also widely discussed over unclassified channels in Washington and elsewhere.

**"WHENEVER THE FULL CONTENTS OF THESE EMAILS ARE LEARNED, THERE IS INVARIABLY LESS THAN MEETS THE EYE"**

The email message about the dead officer was created by a Defense Department official, Jeremy Bash, who at the time was chief of staff to then-Defense Secretary Leon Panetta. It concerned Dario Lorenzetti, a Fort Worth native — later revealed to be a CIA officer — who died Oct. 13, 2012, when an Afghan intelligence officer shot him in the chest while he was wearing a side vest in a so-called "Green on Blue" attack. The email was sent on the day Lorenzetti's death was confirmed.

Lorenzetti's association with the CIA was not disclosed to reporters four days after his death and widely reported in the news. Some of his obituaries listed him as a Special Agent.

"As you'll be hearing," the Bash email began, "a coalition member pulled the ripcord on a vest in front of coalition guys loading a helicopter. Total of 14 either killed or wounded — some U.S., some Afghans. Right now we think one U.S. mil killed and one wounded."



U.S. Democratic presidential candidate Hillary Clinton speaks as her husband former President Bill Clinton and their daughter Chelsea Clinton accompany her at a campaign rally in Des Moines, Iowa January 31, 2016. BRIAN SNYDER / Reuters

The next paragraph of the email, which was released Friday and ~~was~~ posted on the State Department's website, has been whited out and classified "Secret." Officials who have reviewed the uncensored version say Bash was attempting to preserve the CIA officer's cover. But some of the language he used, now that Lorenzetti is known to have been a CIA officer, could be read as a U.S. government acknowledgement that CIA officers pose as State Department personnel in a specific country, Afghanistan — something widely known but not formally admitted. Therefore, the section of the email was classified and ~~removed~~ from public release.

Bash, who was Panetta's chief of staff while Panetta was CIA director, sent the email to four people — including George Little, a Pentagon spokesman who was a former CIA spokesman, and Philippe Reines, an aide to Secretary of State Clinton.

Bash ends the email by instructing Little, the former CIA spokesman, to "please lash up with (blank)" — presumably either the spy agency or one of its employees.

Reines forwarded the email to Clinton State Dept. aides Cheryl Mills and Jake Sullivan, who forwarded it to Clinton. There is no record of Clinton commenting.

**"IF SOMEONE ON MY  
STAFF DID WHAT SHE**

Bash, in an interview, said the email was not classified when it was sent or forwarded and "did not reference the individual's name, employer, nor any identifying description or information."

**DID...THEY WOULD BE FIRED AND THEY WOULD BE PROSECUTED"**

Once the CIA posthumously lifted Lorenzetti's cover, Bash added, "the original unclassified email could be read to confirm the general use of cover, prompting the redactions we now see. But any suggestion that this email contained confirmation about the person or his cover, or any inappropriate information, is flat wrong."

The 2012 email wasn't the only one referencing a CIA officer or program, officials said. The references were indirect, and Clinton made no comment about them, the officials said.

Some of the references to covert intelligence officers, and other discussions of CIA drone strikes, were against classification rules and were "sloppy," one official said. But views are split on whether they were damaging to national security.

It's unclear, the officials said, whether the emails would have provided significant insights to foreign intelligence agencies, if, as many experts say is possible, Clinton's private server was penetrated or hacked.

The messages at issue are part of a longstanding pattern of senior officials at the State Department and other government agencies trying to talk around classified information over email, sometimes unsuccessfully.

What makes Clinton's case different is her use of a home server to transmit emails about government business. The issue has continued to be a factor in her front-running campaign for the Democratic presidential nomination. However, given that the State Department's email system has been penetrated by hackers linked to Russian intelligence, it's far from clear whether the material would have been any more secure had Clinton used State's unclassified email system.

Clinton and her senior aides had access to secure messaging and telephone systems, but they were not as convenient as email.

As the Associated Press has reported, State Department emails previously made public show a history of classified information slipping into unclassified email. Examples have been posted on the State Department's website in response to Freedom of Information Act requests. Although the classified information has been redacted, it is possible to glean insights into the sensitivity from the context.

In emails about the 2012 attack on a U.S. diplomatic facility in Benghazi, Libya, department officials using state.gov accounts discussed the movement of Libyan militias and the locations of key Americans.

An email from diplomat Alyce Abdalla, sent the night of the attack, appears to report that the CIA annex in Benghazi was under fire. The email has been largely whited out, with the government citing the legal exemption for classified intelligence information. The existence of that facility is now known; it was a closely-held secret at the time.

In five emails from state.gov email accounts that date to Condoleezza Rice's tenure as secretary of state during the Bush administration and have been publicly released after FOIA requests, large chunks are censored on the grounds that they contain classified national security or foreign government information.

They include a December 2006 email in which diplomat John J. Hillmeyer appears to have pasted the text of a confidential cable from Beijing about China's dealings with Iran and other sensitive matters.

Large portions of the email were marked classified and censored before release.

Clinton insists she didn't send or receive information marked classified. But she signed a non-disclosure agreement acknowledging that information can be classified regardless of whether it is "marked or unmarked."

---

1A50

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

b3  
b7E

Field Office Acquiring Evidence WF

Serial # of Originating Document 21777 57

Date Received 2-19-2014

From Boswell

(Name of Contributor/Interviewee)

(Address)

Washington DC

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

MIDYEAR EXAM

Reference: Interview Notes

(Communication Enclosing Material)

Description:

☒ Original notes re interview of Boswell

1A50

HRC-1424



ERIC J. BOSWELL

WAE / When Actually Emp Status w/ DoS.

Resigned from DoS <sup>Nov</sup> Oct 2013 [Fall]

Overall responsibility for sec of comm, people, programs, etc.  
for entire DoS.

① SA in charge of 7<sup>th</sup> floor. — security officer  
I name direct oversight  
over Mag.

2009 — no knowledge of p. server  
no knowledge p. email  
no knowledge.

1st aware when news broke in press.  
Found Sec State very responsive to security issues

Show Redacted Memo

drafted early in Administration

Inquiries from Staff about using BB Config  
for Classified

asked Staff to brief on what on possible  
& informed it was not.

Concern over Sec Staff (most came through campaign)  
using BBs on Mahog row. — told to stop & they  
did

No specific instances.

No previous instances.

Not sure Sec State used a work station.

Secure phones & staff w/ all kinds of ways to communicate.

Show of redacted email -

3 days after office

Lon Luciani - ex director of executive sec

Chief Admin Officer.

Stand alone work station - means to Boswell.

a work station not necessarily one off the system.

Dont have recollection of any further discussion.

DS didnt sanction use of BlackB. on Mang Row.

**Kennedy, Patrick F**

**From:** Lukens, Lewis A  
**Sent:** Saturday, January 24, 2009 8:26 PM  
**To:** Kennedy, Patrick F  
**Subject:** Re: Series of questions

[RELEASE IN PART B6]

I talked to Cheryl about this. She says problem is hrc does not know how to use a computer to do email - only bb. But I said would not take much training to get her up to speed.

**From:** Kennedy, Patrick F  
**To:** Lukens, Lewis A; 'habediri'; 'cmills'  
**Cc:** Smith, Daniel B  
**Sent:** Sat Jan 24 20:22:20 2009  
**Subject:** Re: Series of questions

[REVIEW AUTHORITY: Frank Tumminia, Senior Reviewer]

That is why this is the best solution

**From:** Lukens, Lewis A  
**To:** 'habediri'; Kennedy, Patrick F; 'cmills'  
**Cc:** Smith, Daniel B  
**Sent:** Sat Jan 24 19:49:30 2009  
**Subject:** Re: Series of questions

She'll be able to.

**From:** Huma Abedin  
**To:** Kennedy, Patrick F; Lukens, Lewis A; Cheryl Mills  
**Cc:** Huma Abedin; Smith, Daniel B  
**Sent:** Sat Jan 24 19:48:27 2009  
**Subject:** Re: Series of questions

Yes we were hoping for that if possible so she can check her email in her office.

-----Original Message-----

**From:** Kennedy, Patrick F <KennedyPF@state.gov>  
**To:** Lukens, Lewis A <LukensLA@state.gov>; Cheryl Mills  
**CC:** Huma Abedin; Smith, Daniel B <SmithD2@state.gov>  
**Sent:** Sat Jan 24 19:29:25 2009  
**Subject:** Re: Series of questions

Cheryl

The stand-alone separate network PC is on on great idea

Regards

Pat

**From:** Lukens, Lewis A  
**To:** 'cmills'

Cc: Hamed, [REDACTED] Kennedy, Patrick F; Smith, Daniel B  
Sent: Sat Jan 24 19:10:33 2009  
Subject: Re: Series of questions

B6

We have already started checking into the NSA bb. Will set up the office across the hall as requested. Also think we should go ahead (but will await your green light) and set up a stand alone PC in the Secretary's office, connected to the internet (but not through our system) to enable her to check her emails from her desk. Lew

---

From: Cheryl Mills  
To: Lukens, Lewis A  
Cc: Huma Abedin ; Kennedy, Patrick F  
Sent: Sat Jan 24 19:05:24 2009  
Subject: RE: Series of questions

so I have now read up more on POTUS' bb (which appears not really to be a bb but a different device).

[REDACTED]  
is [REDACTED] to her being able to use an encrypted bb like the NSA approved one he has in the vault and if so, how can we get her [REDACTED]

and if not, let's set up the office across the hall for her to use - it needs a phone etc. so she can go across the hall to check her bb.

cdm

---

From: Lukens, Lewis A [mailto:LukensLA@state.gov]  
Sent: Friday, January 23, 2009 6:54 AM  
To: [REDACTED]  
Subject: [REDACTED] of questions

Questions 1 and 2 - yes. Will give you more details this morning

On the bb for hrc, can we chat this morning? I may have thought of a workaround but need more info on her bb use from you.

Lew

---

From: Cheryl Mills  
To: Lukens, Lewis A  
Sent: Fri Jan 23 06:47:59 2009  
Subject: Series of questions

Lew -

who can I talk to about:

1. can our email be accessed remotely through the web using a non-DOS computer like my laptop?
2. I am traveling to the M-E tonight - will my DOS bb work there and is there a cell phone attached?
3. spoke to Dan re: bb for HRC (and reports that POTUS is able to use a super encrypted one which)
4. spoke to Dan re: setting up Counselor office for HRC so she can go across hall regularly and check her email.

cdm

RELEASE IN PART  
B1, 1.4(G), 1.4(E), B7(C), B6, 1.4(C)

~~SECRET//NOFORN~~  
DECL. 03/02/2019

INFORMATION MEMO FOR CHERYL D. MILLS - S

FROM : DS - Eric J. Boswell

SUBJECT: Use of Blackberries in Mahogany Row

REVIEW  
AUTHORITY:  
1.4(E) Barbara Nielsen,  
1.4(G) Senior Reviewer  
B1

We have worked closely [redacted] to review all options that would allow Secretary Clinton, you, and a small number of staff to use Blackberries [redacted]

[redacted] Our review reaffirms our belief that the vulnerabilities and risks associated with the use of Blackberries in the Mahogany Row [redacted] considerably outweigh the convenience their use can add to staff that have access to the unclassified OpenNet system on their desktops. [redacted] 1.4(E) 1.4(G) B1

[redacted] We also worry about the example that using Blackberries in Mahogany Row might set as we strive to promote crucial security practices and enforce important security standards among State Department staff.

As an alternative, we suggest that DS work with S/ES-IRM to make access to the Secretary's OpenNet account on her desktop workstation as easy and convenient as possible. For example, we are happy to work with IRM to lengthen or even eliminate the time-out function to allow the Secretary's Special Assistant to log-on to review her emails and schedules.

[redacted] While we cannot recommend using Blackberries inside the Mahogany Row, we do not want to stand in the way of issuing Department Blackberries to the Secretary and her senior staff for use outside Mahogany Row. Those Blackberries can be synchronized with your OpenNet Microsoft Outlook accounts, provide full cellular, e-mail, and internet functionality, and provide unclassified mobile technology when you are away from Mahogany Row. 1.4(E) 1.4(G) B1

I cannot stress too strongly, however, that any unclassified Blackberry is highly vulnerable in any setting to remotely and covertly monitoring conversations, retrieving e-mails, and accessing calendars. I am attaching reports from DS's

~~SECRET//NOFORN~~

Classified By: DS - Eric J. Boswell

FOUO 17958 Reasons: 1.4(c) (1) and (2)

~~SECRET//NOFORN~~

- 2 -

Office of Computer Security's Cyber Threat & Analysis Division that give further background on those risks. [REDACTED]

1.4(E)  
1.4(G)  
B1

If, after considering the vulnerabilities that I describe above and the alternatives that I propose, the Secretary determines that she wants a limited number of staff to use Blackberries in the Mahogany Row [REDACTED]

1.4(E)  
1.4(G)  
B1

Attachments:

Tab 1 - Excerpts from DS/CS/CTAD Reports on Blackberry Vulnerabilities

Tab 2 - [REDACTED]

Tab 3 - New York Times Article: "Obama's Pbone Security and Yours"

Tab 4 - Washington Post Article: "Your Cell and Your Berry: Tools for the Enemy"

1.4(C)  
1.4(E)  
1.4(G)  
B1

Eric J. Boswell

Assistant Secretary for Diplomatic Security (1996 to 1998, and 6/2008 to 12/2012) –

Director of the Office of Foreign Missions (DS/OFM) (6/30/2008) –

Assistant Deputy Director for Security ODNI (2005 to 2008)

- Introduction

- Voluntary / Can stop at any time ✓
- NSLB Disclaimer re: Garrity / not interested in prior statements to DOS
- FBI's interest in this matter is to assess whether classified information was stored or transmitted on the server and if it was compromised by either authorized or unauthorized users.
- Discussion of classified topic, if necessary

- Brief overview of duties

- What is your current position?
- What were your duties at DoS?
- What were your duties as the A/S of DS, as relevant to the security of the Secretary's communications?

- Knowledge of the private server, email system, and other devices?

- Did DS have any role in the set up, or maintenance of the server?

• If so:

- What was there an approval process for the use of private email / email servers?
- What steps were taken to review the risks / benefits of this arrangement?
- Who was involved in the review process?
- Was this consistent with DoS policy at that time?
- Did the server violate department policy as stipulated in the Foreign Affairs Manual?
- What is the current policy today?
  - When / why did it change?
- What role did DS play with respect to providing secure communications to Secretary?
- Did DS provide any guidance / recommendations on the use of devices?
- What secure comms were available to the secretary at her home and when she was traveling?
  - Phone, Fax, Email (Classnet / JWICS)

- Discussion of Memo

- What was the context of this memo?
- Who requested to use BB on Mahogany Row?
  - Had this been done by previous secretaries?
  - Why did she need her BB on Mahogany Row?
  - Do you (or DS) know of requests made by Cheryl Mills for a standalone system that wasn't on the DoS network?



- It appears that the issue is connecting to private server / email from DoS. How was this resolved? – i.e, BB on Mahogany Row, separate computer system, other?

○ Can you please explain the last paragraph?

- *If after considering the vulnerability that I describe above and the alternatives that I propose, the Secretary determines that she wants a limited number of staff to use BB in Mahogany Row [redacted]*
- What was the Secretary's decision?

○ References to Office of Computer Security Cyber Threat & Analysis Division

- What were the primary threats facing DoS at that time?
- How was threat information relayed to the Secretary and her team? Memo / DS.
- Are there any specific threats that you recall? *Individual or Mass Memo*
- Were there any other issues or concerns regarding general security posture of the Secretary and her team? (i.e., Egregious actions, not minor infractions)
- Who was the primary POC in the Office of Computer Security Cyber Threat and Analysis Division at that time?
- How does Office of Computer Security fit in to world of IRM, IRM-S/ES, PACE, etc?

- Is there anybody else that we should talk to regarding this matter?
- Any other thoughts / concerns regarding this matter.
- NDA request

*one is security side  
one is IRM.*

*DS tests systems  
tries to ID  
classified*

*job to detect  
breaches.*

*pushes  
out info*

*Spies fishing  
Hostile Govt.*

1A54

FD-340 (Rev. 4-11-03)

File Number                      302

Field Office Acquiring Evidence WF

Serial # of Originating Document 61

Date Received 12/22/15

From Bryan Pagliano  
(Name of Contributor/Interviewee)

Washington, DC  
(Address)

By SA                       
(City and State)

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

1A54

MIDYEAR EXAM

Reference: 302  
(Communication Enclosing Material)

Description: ☒ Original notes re interview of

- Bryan Pagliano interview notes  
- Documents displayed to Pagliano

1

12/22/15

Background

[redacted]

b6  
b7C

2006 - Senate campaign → Presidential

↳ Director of Presidential campaign

↳ After, archiving, wiping & reinstalling

Talked w/ Capricia Marshall (friends of Hillary)

b6  
b7C

+ Ali Rubin about working for state)

b6 Per  
b7C DOS

~ early 2011

[redacted]

[redacted]

at SD → wrote performance reviews/weekly mtgs

moved into

Not hands on at SD - did not have admin accounts

his place

↳ Mostly writing recommendations/memos

2012

↳ mostly mobile computing, small branch for BBs

b6 Per  
b7C DOS

[redacted]

had issues at 1<sup>st</sup> then turned into good program

transitioned out

↳ ITTI program

b6  
b7C

[redacted]

[redacted]

(current employer) around that time interviewing

Fall 2008 JC w/ Pres Clinton's office (from WH) + personal affairs

was Mac OS X G5 or G4 → called or emailed him on HC email. Heard about liquidation of

Email Server

issue w/ uptime  
not stable

equipment. Can sell him eq. 1950, 2000, UPS, FW, etc.

↳ Asked for help setting up equipment

Bought Microsoft SBS 2008, BES, A/V, Syslog server, 515E PIX

↳ JC skill level at time - yr 1 or 2 Sys Admin

Weekend trip

Installed server in Chap, NY. New he had 2008 email setup

March 2009

↳ took all user names + passwords. Pull popmail to Outlook client  
into Exchange server

Part of migration on site. Finished off site

HRC-1456

12/22/15

March 2009 - Equipment:

Airport

Printer (HP) - support IPP (port 9100). Opened it up to internet

they could print from Hailam Office

b6  
b7C

had physical access but not admin

OSX Server - G4 or G5 → later <sup>intention was</sup> got installed as a workstation

12U Rack - BISE FW

Dell unmanage switch

PE 1950

PE 2900

3U Power supply

3TB hard drive

No tape backups

Disk to disk backup so they could do backups

Mac OSX

Optimum ISP - bought internet from AboveNet

When migrated mail, would have chosen not to keep a copy on old server

2 Domains - presidentclinton.com & clintonemail.com

b6  
b7C

→ Pointed both to 2900

JC provided

Justin, Huma (didn't migrate at 1st)

accounts/passwords

→ Did not migrate Hillary's email to new server

New - everyone had access to either domain for receiving email.

- Reply address set as clintonemail.com

12/22/15 SBS Setup

Email only

Behind Firewall - only server

[redacted] - tech interviewed - talked to him about Sharepoint Site b6  
b7C

or JC - said it was a migration but didn't appear to be used

(campaign - Pre) PE - used as SQL server

1950 - 20-25 servers on campaign in Ballston

↳ may not have wiped them b/c staying w/in the campaign

↳ For rest of servers, did a RAID reconfigure / bit "wipe"

No file access. Sharepoint was turned on but appeared no use.

password = Forefront was 2nd choice

[redacted]

Main server - Ran Microsoft tool to turn off services b7E

- Windows Firewall

- Forefront. Wanted to use Postini (cloud filtering)

↳ JC didn't want to use Postini (didn't like cloud)

↳ was not stable on SBS until ~2010

Just doing

DNS (not

DHCP)

- scanned mailboxes & then acted as virus scanner on Windows server

- MS backup service → start w/ external HD

Don't think he

did WINS

1st in, 1st out

↳ schedule - full 1x week, differential every day

- WSUS - automatic patching & reboot overnight

FW Filtering

Inbound

filtering. Talked

to SS guy

he recommended

filtering

Remote access was BFA. Set up Windows server logs to alert JC

every time of failed login attempts. Just do IP filtering b6  
b7C

↳ led to discussion of upgrades

↳ sent to his blackberry account

w/ IP address, username, false

Do IP blocking. Some accounts

2nd Server - Windows 2003 - MS Virtual server w/ BES

↳ before upgrade in 2010

- Kiwi Syslog server on it - Collected FW logs HRC-1458

↳ Didn't get a chance to review them

- Only looked at them ~ [redacted] h. JC wouldn't have

12/22/15

The one ← Utility server Telnet was on server (console access)  
that was exposed → 2003 server <sup>virtual</sup> <sup>as workstation</sup> was used initially to migrate mailboxes

↳ RDP Thought JC didn't know how to login to mailbox

Tested ← ASA Cisco. Tried to do 2-factor authentication for RDP only  
it but wasn't reliable so didn't shut off RDP & only used RDP

Use local account on Utility server to remote into Exchange Server

JC & BP's workstation - Certs on machines, RDP 2<sup>nd</sup> level auth

BP - sent a lot of screenshots to JC about how to set up accounts

Summer 2009 - noticed an account that said "H"

- hdr (3 #s) hdr22@clintonemail.com  
or hdr17@

Can receive on either domain proclinkclinton.com  
or clintonemail.com

Summer 2009 - [redacted] or [redacted] (unclear)

- both Foreign Service officers, knows a lot of IT

IRM under Mgmt Bureau. IRM on 7th floor [redacted]

↳ BP for everyone else

They called him into the office & asked about the clintonemail.com domain

Relayed the ← [redacted] had conversations about the server. Expressed concerns about  
convo to [redacted] the server being used as records retention. (couldn't get them to inner O' (unsure))

BP - Scheduled mtg w/ CM about the issue - late 2009, maybe 2010

CM - cited conversation or something Colin Powell said. Don't let them take your email away. This is ok.  
↳ [redacted] (sp?) assistants to CM.

Later conversation w/ [redacted] about security concerns

[redacted] propose TLS tunnel b/w State Server & Server in Chap

↳ assumption was that it was only for personal use

b6  
b7C

b6  
b7C

b6 Per  
b7C DOS

b6  
b7C

[ ] got involved:

12/22/15

① Issue where client email was not getting delivered to State.gov

② When internet connection got knocked out b/c storm (optimum)

Vendr - US21 Inc → invoice JC directly

2009 - more b/c setting it up

2010 - hardly any work done

2011 - spiked again b/c of 2<sup>nd</sup> install, more technology

2012 - Spiked a little b/c of transition

Intrusion attempts - alot of BFAs. See IP + username attempted to logon. generic u/p

BP did not have an email account

If user they recognized, ask if there were login problems

USB drive failing - left it behind the server in the rack

2011 Summer? Transition to NAS - move them  $\frac{1}{2}$  for backup [60/40 or 70/30]

① Cisco NAS

- just pointed the backups to the new NAS

② Managed Switch -

- offloaded the syslog to the NAS

- for ISSI

③ ASA FW 5500 - security upgrade - Cis botnet filter bought - helped w/BFA

↳ had to go thru

- Intrusion Protection Service (IPS) from Cisco

FW to get thru to servers

BP - JC had more flexibility to create accounts

Export of archives [ ] wanted his email (never deleted email)

Export of [ ]? (not sure)

Import Humm's contacts from state.gov account

12/22/15

## SBS Environment

↳ Devices → no visibility

↳ Monica talking about a laptop - started to talk to her around 2012

↳ BB HC used bought in 2008 - that broke

↳ Monica said she liked it + wanted the old model - found 4 phone

↳ JC on trip

↳ "We" activated the mail ~ Winter 2011?

↳ Monica gave impression that there was a laptop being used

Mailbox scanning document - coming out of Forefront - Virus scanning  
assume it was

Exchange log

JC - handed him usernames + passwords, but would not have had  
Bryan admin password

- He did setup 3/9/2009 Install under Administrator account

- He did upgrade

- He did not do uninstall

Conf call b/w [redacted] JC - wanted a more robust system

Then [redacted] CM got involved, then [redacted]

Convo with CM about security of the system - B+ on security

[redacted] decides on PRN

Blue sheet #11 → "clean up" → If you delete a msg or more mailboxes, the  
[redacted] doesn't decrease in size. Built-in "cleaning" function [redacted]



12/22/15 Winter storm of 2011  
Sandy = gmail accounts

- told JC advice, can change her records to set server at Chap to 10 then gmail to 20, when I can't find 10, go to 20
- Huma + HC likely, but JC would have done this
- Didn't have admin access
- Google for business - push to a domain

Back up document → Would have been backed up to NAS-2013

July 2014 - phone call w/CM & PRN

b6  
b7C

July 2014 - HC - thinks it was [redacted] (engineer on HC campaign)  
He used a reg. Expression text editor

Summer/  
Fall 2013

Convo w/ [redacted]

→ questions of how to work w/pst files  
context of Benja 2

b6 Per  
b7C DOS

→ questions on sorting emails, searching  
→ asked details on timestamps

↳ wanted to know what would happen to date stamps if opened a file (modified date)  
or if it moved file

↳ she didn't want to give impression that she was modified

↳ Assumed PRN gave her a pst to work with

July 2014 - CM & PRN

- explain the "gap" of emails
- individuals that received emails from her address prior to the emails PRN was able pull

12/22/15 "Gap" in emails - July 2014

- ↳ Found out From JC there was a BB using BIS/BIZ
- ↳ AT&T BB - prior to the one JC setup on the system we built
- ↳ only other place to look would be on the file system itself

Call/Talk w/ CM - Fall 2013

- ↳ had convos about archiving data & repurposing machines
- ↳ Botten Nuke ⇒ He used before. But can't recall the tools.
- Explaining what type of deletion process to use when repurposing
- She explained what PRN was proposing to use
- Explained difference "bit" wiping & just deleted
- She was being told by PRN

Call w/CM - Spring 2015

- ↳ would you talk to David Kendall, JC talked to him
- ↳ Told DK shorter version of story

b6  
b7C

[redacted] would check in on him every once in a while - Not advising

Conf call w/security team - 1/11/2011 - Maybe call w/ [redacted]  
- Re authentication & filtering

b6  
b7C

HC-014 [redacted] Contact at USZ1

b6  
b7C

HC-014 BES IT Security policy - reding of the policy, Restricting Bluetooth

HC-023 [redacted] - pushed security policies individually

b6  
b7C

HC-001 Nov 28, 2011 payment - Cisco VPN (2-factor), power outage on 8/28

- moved NAS to [redacted] server

HC-002 - Configure VPN - no user VPN, j [redacted]

HRC-1463

- IPS went in place when Cisco ASA went in
- tuned it over time. Turned on logging mode
- Some point turned it off logging mode

12/22/15

mailbox wickoff - was for [redacted]

b6  
b7C

HC-004 Push security policies for iPad - probably for HRC

↳ He did not configure it for her

Patch for BES server

↳ saw the email address

↳ Does not know if this was a new device

HC-010 Jan 2013

↳ Potential "H" email issue Jan 2/2013 - 3/2013

↳ could have been when dealing w/Monica about 4 RBs

↳ Rec. for CM. Document the state & where we should be going

↳ sent in email [redacted]

b6  
b7C

↳ only CM accounts are gmail, state (old NYU)

HC-012 July 2013

↳ Msg delivery failures - no specifics

↳ conf calls w/ [redacted]

b6  
b7C

12/6 10:15am



b6  
b7C

2006 Senate (Cappi) ramping stuck around to as Cappi.

Cynthia Marshall HICPA - Interviewing at State Department cited for 4 yrs.

b6  
b7C

No admin record at State. Under memo advocacy for progress.

State - mobile connectivity. [redacted] [redacted]

[redacted] to [redacted] early 2011.



b6  
b7C

Fall 2008

JC with BC for some time. Called me. Email introduction. I know that

you're liquidating equipment. We have a server we are transitioning from.

2950, 1250, 1250, UPS, switch, firewall, no software. Didn't know HICPA would be

SoP. I did work street we had anti-syslog, config pix 515E, export Forefront.

Mac OSX server running open source software. People starting to use.

- JC year or 2 sys admin skills.

Taking user names, pass word JC gave me - pop mail from Mac to Outlook client.

JC, re, UPS off - Physical equipment in - some equipment started to break, but continued in my hotel room. March 2009

Apple G5 or 4 tower - Airport (firewall), printer HP and support 1PP - opened to internet to print, desk side out.

1pt in 1250 Bell - ed with 1950, 2950, 30APC power supply,

2950 - 1TD hard drive - disc to disc back-ups - couldn't rotate tapes

HRC-1465

No KVM - One generator for the house. Cable modem. Optimum - bought a tract from the act.

App Server - Don't know other functions.

Migrate AS - PS - 2 domains - pres.chiba.com & clibachanal.com

Archie: [redacted] JC, Hanna had sent didn't <sup>move</sup> [redacted]

b6  
b7C

- Didn't know if there was a Hilkey Account but didn't migrate from JC gave direction.

- On New server - could receive on both domains only send from.

[redacted] or JC could monitor printer but I don't know.

b6  
b7C

[redacted] had physical access - hard drive failed on utility and he did it. Now JC Don't know who installed AS. JC had admin access to AS.

No known upgrades for AS.

After AS migration - we discussed repurposed. <sup>JC</sup> How reinstalled as a workstation. somewhere in Ch. Also used as a work station the 2nd time I went to Ch. In basement.

- Don't know how users connected to AS.

Changed DNS and MX records. Nothing to AS anymore after weekend.

When I moved, would have popped out - No distinct memory.

Discussion with JC about moving to basement. Only one internet connection.

Didn't want to. JC wanted to have physical access to servers  
- more reliability.

BP server - Function of equipment prior - email system. Microsoft. Poweredge was original server. 1950 - don't know. Copying HQ YMCU W. Foster Drive. Data center air - conditioning.

- 2950 and 1950 - may not have wiped. Used RAID utility to wipe disks. for the rest. Prob. good practice

HRC-1466



Blaine

- Disc / Mailboxes not migrated.
- 2 factor. On ASA stated to do. expected with. Put it on 2 workstations.
- Blaine JL. My idea. RDP showing weaknesses. Good practice. It currently remotely.
- JL was same to 2 factor. Wanted RSA Secur.
- I would try to talk to JL. We evolved. He understood more later.
- Domain: clinton email, pro clips. Didn't do DNS management.
- JL changed MX records.
- trained JL on system.
- In summer of 2009, I noticed an account that said H. I asked JL what this is. He said Hillary. I received personal email.
- HBR 22 @ clinton email.com
- Changed to Fred 109 after Sid Plummer.
- In summer 2009, met [redacted] at [redacted] 6th FSO. b6  
b7C
- brought us to 7th floor. Do you know about clinton email.com domain.
- Don't know how he knew about email. Ext relationship with [redacted] since. Didn't kill down in first meeting. Relayed to [redacted] via email.
- 2nd conversation - we at server being a record retention issue. Can't get through to inner circle. - can you? late 2009 maybe 2010. I raised issue with Cheryl Miller. She said other JCS had done. CP said CP had done. Person to person in her office. Weeks between meeting.
- [redacted] didn't want to know anymore. I say has returned to JL. b6  
b7C
- 3rd conversation with [redacted] - security [redacted] travel with OOS - in Chicago - Didn't talk to anyone.
- 'It be [redacted] if classified information wasn't being transmitted.' Don't know who wrote it. Didn't know what prompted him to raise it - thought email was personal.
- Through CM assistants.
- ce.com wasn't being delivered to state. you [redacted] got involved. b6  
b7C

- optimum connection went down for sandy. Couldn't get second connection not feasible.

Hardware paid for Carter family campaign. Would with US21 equities.  
would invoice JC directly.

N. contract - No scope - came with JR. He wanted retainer, but I did hourly. 2009 - stand-up 2010 - hardly anything. 2011 - second install 2012 - transition

Once at Oak, 2008 - didn't know install - I did know. Hur b

Server never in another location.

no security breaches. A lot of DFAs. we never were & close. No email acct. Post admin. Only [redacted] - it was then.

- no giant spikes through AHA

email: ex 400 to NARS. ~~Ex 400~~ failing. CISCO makes good products. May have

corrected w21. Nov 7. More than half to back-up 60/40 to back-up

over to file. Unplug USB - pointed to NAS. we back-up to NAS

End upgrade June 2011 - added memory & -1.0. CISO WAS

Gigswitch, ASA firewall, blocked <sup>5560</sup>gigswitch, WAF, more toward  
firewall up/ides. BFA's were non-targeted at random. Thought better so

bought botnet filter thru CISCO. Also did intrusion protection,

replaced batteries on UPS. Upgrades, maintenance.

check on BES for software patch. In 6/11, user from BES 5.0 to 6.0

1 did upgrades picking 6.4Ks - JL to users.

Use accounts:  $\pi$ . Can't remember.

2 adams - 12 ad re

~~He~~ Import. Export - [redacted] wanted his exact when leaving. 4068.

May have done   for export. Nitrate.

Import Home-state.gov contacts to server.



- Show acct: 4/8: Don't recognize all names. Don't know how archive after by poll boxes - I don't know.
- Ways connected: inside fire wall was me. Any client they wanted to be open to them.
- Clouded memory - Monica talking about a laptop. That was downloading Outlook email.
- HRC had 2008 b6. Met with M.H. in 2012-12 tried to contact b6.
- No migration between HRC. Account name changed.
- Mailbox scanning - shown - out of function - scanning for viruses, not likely.
- Would've talked to JC about DFA of Bethot theory. No countries stood out.
- Didn't know identified. No one ever told me.
- Never accessed content on server.
- Ex time stamps shown - 3/01 - initial meeting. JC had passwords not by admin.
- 8/12 - service pack upgrade.

PRN transition - [ ] doing her own thing. [ ] JC 3P talks about future of server.

b6  
b7C

More people get involved [ ] CM. Not sure of [ ] interest.

JC got requests to add. We had limitations. Spoked discussions.

[ ] gets involved. Don't know how [ ] handled. She looked for vendors. Presentation - 3 candidates. Asked for opinions. I said PRN.

b6  
b7C

[ ] made ultimate decision to PRN.

b6  
b7C

- Arch details to PRN - giving passwords. Details.

- [ ] Wasn't in Chicago - a.

b6  
b7C

- Convo [ ] Talked once, twice.

- Clean-up - Exchange - clear out white space. [ ] email box.

b6  
b7C

Winter 2011

~~Hurricane Sandy~~ - ISP had no power. Time was going to take [redacted] le.

I suggested to get server at Chappaque 10 and Gmail to 20. NAS record goes to gmail. Not sure who he set-up. Squelchy deals. case Hama and Hurray. So most likely. didn't push the buttons.

gmail for business - can't push a whole domain.

NAS had 500GB - target could've been either. Based on time NAS.

PRN No involvement in their selection. We talked cloudjacket, 2factor.

Maybe [redacted]

- JATTO heard in conversation. [redacted] what they should do.

- 07/2014 - archive email options -

- 07/14 - email - [redacted] engineer from Hurray copyright.

- Conversation with [redacted] - details how to work with PST

files. How do time stamps happen? Response [redacted] summer

to Fall 2013. Sorting through. Hopening [redacted] sage modified step. She didn't want to give impression that [redacted] Probably from PRN.

- BP, CM<sup>PRN</sup> - explain gap in emails. Individuals [redacted] prior to what PR was able to pull. In conversation with JR - found out blackberry before mine. Gap in [redacted] 2009 + March 18, 2009.

- No other memory with BP, CM PRN convo after.

[redacted]

Fall 2013, CM calls and says PRN was going to retire. Using 2 vendors. PRN would have used.

Spring [redacted] CM would you mind talking to David Keadell - I did. Before counsel. Shorter version of this. Noting I told him that I didn't tell you.

HC-001- 3/30/2007- includes expenses. rental car.

6/17/2011- expenses

lost check. Nk'd in to report payment.

HC-014- cont call security team - [redacted] outbound filtering.

b6  
b7C

[redacted] is contact at US21.

- Rec confy for BB - S/S turned [redacted] the room except Justin. Maybe [redacted]

- Justin could wipe or restore a device that was lost.

HC 023- [redacted] - one by one

b6  
b7C

HC001- 11/28- CISCO VPN, Power outage, patching BES, NARS sys log.

HC002- VPN- Efactor solution not just RDP. Didn't do VPN.

IPV when AIA

HC008- mailbox link-out - [redacted] export mailbox. Fix corruption.

b6  
b7C

- Talk to [redacted]

HC 004- S/S I pad. I didn't configure. Don't know when she started using it.

You could see what email account.

HC006-

HC 010- rec for CM - analyze [redacted] security. B+ grade. What can we do.

where we need to go. I'm not trying to take you there. CM has state  
at gmail. NYU she abandoned.

- Next entity to support.

HC 012- md failures - don't know.

- cont calls - [redacted]

Network & Tech for cluster bandwidth

b6  
b7C

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1353814-0

Total Deleted Page(s) = 5  
Page 14 ~ Duplicate;  
Page 15 ~ Duplicate;  
Page 16 ~ Duplicate;  
Page 17 ~ Duplicate;  
Page 36 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

#60

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

73

Date Received

5/24/2016

From

HEATHER SAMUELSON

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A60

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

HEATHER SAMUELSON

DOCS SHOWN TO SAMUELSON

HRC-1761

5/24/16 3:50 PM

HEATHER SAMUELSON

BETH, ALEX, HAN



①  
b6  
b7C

CURRENT PERSONAL ADDRESS TO THE SA  
DDS JOG - MARCH 2013 WH LIAISON OFFICE  
Assistant → HEAD OF OFFICE  
MARCH 2014 → 1 YR WH CONSL OFFICE

- INTERACTED W/ CHIEF, NOT W/ S. VERT OFFER.
- IS/SCI (STILL HAS IT TODAY)
- REINVESTIGATION WHEN LEFT THE WH (IN 2014)
- REMEMBERED TRAINING, BUT NOT THE DETAILS.
- ALSO TRAINING @ REINVEST
- NONE OF FOIA, FED RECORDS ACT → NOT AT STATE BUT AT WH ON PROS, RECORD ACT
- OUT PROCESSING AT DDS → NO GUIDANCE ON INFO TO RETAIN
- CORRESPONDED ON STATE.GOV ACCOUNTS
- DIDN'T KNOW PRIVATE EMAIL UNTIL SERVING AS PRIVATE ATTORNEY
- SERVICE → VIA KNOWLEDGE AS ATTORNEY
- ONLY GOT 2 EMAILS WHILE AT STATE - BDM, GARDEN

REVIEW - CHERYL'S OFFICE (FRIENDSHIP HINTS)

- PRN NOT INVOLVED IN PRN TRANS. → VIA REPR
- ADHOC (NOT CONTEMPORANEOUS)
- NO KNOWLEDGE AT THE TIME, ONLY VIA REPRESENTATIVE OF THE SECRETARY
- HRC OFFICE LOCATION OF LASTOP / THUMB DRIVE → NO KNOWLEDGE
- KNOWS SHE CHANGED EMAIL
- UNDERSTANDING IS NO EMAILS WERE TRANSFERRED A NEW ACCOUNT FOR HER
- DON'T KNOW HOW

# (DOS REQUEST FOR EMAILS)

②

late 2013  
July/August 2014

- INST IN INITIAL DISC.
- A [redacted] TO ASSIST CHERYL
- CHERYL SPOKE W/ THE DEPARTMENT  
10/20/2014 LETTER FROM <sup>US</sup> KENNEDY TO CHERYL
- NO SPECIFIC DATE
- NOTICED GAPS IN RECORD KEEPING → H.C. & OTHER FORMERS FOR RECORDS IN THEIR POSSESSION
- NO GUIDANCE FROM DOS THAT HS IS AWARE OF
- WAS H.C. REQUESTED TO SORT WORK/NOTWORK  
(HS WAS ON)  
→ CALL IN LEGAL ADVISORS AT STATE FNU LNU
- SEC REPR [redacted] JATION - DAVID KENDALL & OTHERS FROM W/C

Collection  
FROM  
PRN

[redacted]

WAS ONLY PERSON H.S.

b6  
b7C

SPOKE W/

- JAN 2009 - FEB 2014 → REQUESTED ALL EMAILS
- JAN 09 - MARCH 09 - ASKED PRN TO DOUBLECHECK BUT THEY DIDN'T HAVE THEM
- UNDERSTOOD ALL EMAILS ON BB AND NOT ON A SERVER → NOT RETRIEVABLE
- GOOGLE/HURRICANE SANDY → DID NOTICE A FEW EMAILS W/ [redacted] @GMAIL, LOGGED IT AND ONLY FOUND 1 EXCHANGE
- OLD APPLE SERVER - NO CONTEMPORANEOUS KNOWLEDGE
- ASSOC/MT → NO DIDN'T REACH OUT, DID KNOW THAT SHE MIGHT HAVE ANY DOCS
- NOT SAVED ELSEWHERE (NOT ON SERVER/LOUD, ETC)
- [redacted] SENT LINK, DOWNLOADED FILE → PUT ON CDROM FOR HS

b6  
b7C

b6  
b7C

John Deffe

(3)

## GOV EMAIL TRANSFER

- NOTHING IN POSSESSION ALREADY BEFORE CONTACTING PRN
- NO INFO FROM PRN ON LOCATION OF FILED EMAILS <sup>LIVE MAILBOX</sup> ~~ARCHIVE~~ WERE FROM JUST "AND RESENTS"
- SAME PROCESS TO RESEND FILES

- (1) GOV FILES - END JULY / EARLY AUGUST  
Full support
- (2) ALL EMAILS (TOOK GOV)
- (3) WANTED GOV BACK (SOME MISSING)
- (4) GOT MINI PETS THAT WERE MISSING

• LINK VIA EMAIL → [ ] LOGS ON TO COMPUTER

b6  
b7C

DOWNLOADS FILE → PW PROJECT (TOLD HS. VERBA)  
IN OUTLOOK

• [ ] → IMPORTED IT INTO OUTLOOK → wasn't working.

• DON'T RECALL NAMES OF FILES / LOCATION ON COMPUTER

• DON'T RECALL DISC OF ENCRYPTION, ETC.

• DID MAKE THUMBDRIVE OF EMAILS PROVIDED TO D.O.S.

• OTHER DATA SETS → ONLY EMAIL ACCOUNT

• DIDN'T CONSIDER USE OF E-DISCOVERY TOOLS FOR THE REVIEW.

LENOVO YOGA 2 → IN BOTH'S POSSESSION (SILVER)

↳ ONLY USED IT FOR REVIEW

2ND COMP B/C SPILT ~~WATER~~ WATER ON YOGA 2

↳ WAS LOADED W/ EMAILS PROVIDED TO D.O.S.

IN FBI POSSESSION FROM W/CONNOLLY.

PC {  
• LOOKS LIKE COMPUTER (SILVER)  
• "HCPRIME 2" USB - ~~DOESN'T~~ DOESN'T KNOW  
• USB THUMB DRIVE - " " "

- BOTH PERSONAL LAPTOPS BUT FOR WORK RELATED MATTERS.

- WIFI AT CHERYL'S OFFICE & AT HOME

- YES - ANTI-VIRUS

- DIDN'T RESURPOSE

- FACTORY RESET (BREAK REQUIRED)

HRC-1768



(4)

## FACTORY RESTORE

Comp 1 - YOGA 2 - FACTORY RESTORE CD 'NO'

b6  
b7c

~~WIFE~~ - JAN 2014 - [ ] REMOVED PST FROM LAPTOP  
KEPT USING AFTER WATER SPILL -> NOW DOESN'T POWER ON  
DELETED IN COURSE OF WORK, BUT NOT ATTEMPT TO 'WIPE'

Comp 2 - NO 'WIPE' TO REMOVE WORKING COPY (IN OUTLOOK)

U/S KENNY

DOS -> DELETE CLASSIFIED ON COMPUTER

RETROACTIVE CLASSIFIED - DOUBLE DELETE

MAY 22ND 2015 -> 1ST RELEASE

THUMBDRIVE W/ PRODUCTION SET WAS IN KENDAL'S  
POSSESSION EMAILS NOT DELETED

PRN - NO DVD COPIES TO HIS KNOWLEDGE

DOS "RESTORE ACCESS" DON'T RECALL WHAT  
THAT MEANS, DOESN'T REMEMBER LOSING  
ACCESS

• GOU

• PRINTED ALL, REVIEWED FOR PERSONAL CONTENT  
ON PAPER

• CHERYL & DAVID REVIEWED ALSO

- TOOK WEEKS TO REVIEW, DON'T RECALL WHEN IT  
END OR IF PRIOR TO FULL SET FROM

↳ NOW PRODUCTION ~~SHIPPED~~  
PRODUCTION -> DOS

## FULL ARCHIVE

• TO ENSURE FULL PROTECTION BEYOND GOU

• REPOSITORY OF FULL -> NO IDEA ON SOURCE

• ~~DO~~ DON'T RECALL DUPLICATES IN DATABASE

• ACTUAL DIPS TO DOS -> EMAIL CAME UP IN  
MULTIPLE SEARCHES

• IF JAN 24, PULLED IT. BUT NOT REGULAR

PRN DIDN'T HELP W/ D UP REVIEW

= REVIEW HRC ARCHIVE?

↳ DIDN'T KNOW WHERE IT WAS FROM

→ FULL SET LATE SEPT / EARLY OCT?

= SAME COMPUTERS AS BEFORE

POST TO CM COMPUTER? → CAN'T SPEAK TO

FOR  
GOV OR  
FULL

= DON'T RECALL NAME, DESCRIPTION OF FILE

= NO COPIES OF THE FULL EXPORT THAT SHE RECALLS

• DO [REDACTED] LESS

• E.I. [REDACTED]

= DIRECT [REDACTED] MAILBOXES ON SERVER

NO [REDACTED] NOT AWARE OF OTHERS

= NO ACCESS TO THE SERVER (OR ANY OTHERS)

= REVIEW [REDACTED] AGENTS OF THE SECRETARY / INQUIRY

LATE SEPT / OCT → PROVIDED TO DDS 12/3/14

FINISHED NEARLY DAY BEFORE

- SAME LOCATION & EQUIPMENT AT GOV REVIEW

- PRINTED IN OFFICE, MIGHT STILL BE IN OLLERY'S OFFICE  
NOT SURE (BLAND - ??, WAS BIG)

- NO ACCESS BY NON AGENTS

METHODS  
OF REVIEW

- GOV TO / FROM → PRIMARY PATH FOR WORK

- FULL EMAIL ARCHIVE FROM TENURE

1. MIL

2. Dpt, A/S, U/S, AMB, Policy Board, Sr ADOS

3. SENDER / RECEIVERS → COR Foreign LEADS

4. KEY WORD SEARCHES [REDACTED] t check

Ag. Libya, Benghazi [REDACTED]

4. → Bill Burns (SUSPECT) → [REDACTED]

1. → Doctor → NOT WORK

6

- PERSONAL → TO/FROM SUBJECT

- LOOKED AT EVERY EMAIL IN THE BOX

"LAID EYES ON" DIDN'T READ IF IT WAS OBVIOUS

HS/DAVID/CHERYL → DEVELOPED PROCESS  
CHANGED? - NOT SURE HOW TO SPEAK TO

INDIVIDUALS CONSULTED W/ NOT AGENTS → NO

NO REASON TO BELIEVE CLASSIFIED WAS  
IN MAILED BOX. NOT MARKED AS SUCH.

→ DISC ON HOW TO HANDLE IF FOUND → NO E/C  
DIDN'T THINK ANYTHING WAS CLASSIFIED.

HUMA EMAILS → SUBJECT LINE, HER ACCOUNT  
WAS <sup>PRIMARY</sup> FOR FAMILY RELATED MATTERS AND NOT  
RELEVANT. BUT WOULD LAID EYES ON.

- AWARE EMAIL WAS CHANGED IN 2013

- NOTICED HEADLINE WAS STOPPING TO SEND BUT DIDN'T  
HAVE ACCOUNT AT TIME - ASKED [ ] WITH - DIDN'T <sup>b6</sup>  
UNDERSTAND RESPONSE, NO RESOLUTION, <sup>b7C</sup>  
NO ONE ELSE CONSULTED.

REESTABLISH CONNECTION IN 11/12/2014

- NEVER LOST CONNECTION, ASIDE FROM ASKING  
GOU BACK.

USED GOU AS BASE AND ADDED FILES  
FROM FULL FILE TO CREATE PRESERVATION

NOTICED GOUS IN FULL, NOT IN GOU SET.

DOC10

DIDN'T RECALL WHAT IT WAS ABOUT.

DOC11 " " CAN'T SPECULATE ABOUT.

DIRECTION TO PRN <sup>→ would delete 7 columns in the mail.</sup> ⑦  
12/2014 → EMAIL TO GODDAYS RETENTION <sup>on one when they were deleted</sup>  
- DIDN'T DIRECT PRN TO REMOVE EXPORTED FTS  
ON SERVER  
- " " " " MAILBOXES ON SERVER

Additional

- NO REVIEW BY NON AGENTS.
- HS PRINTED
- PPT PROVIDED TO FBI
- HS CREATED PRESERVATION COPY ON THUMB DRIVE TO DAVID (BEARING IT WENT TO FBI)
- NAME - DIDN'T KNOW.
- 2ND COPY FOR HS ATTORNEY'S TO KENDALL ALSO. <sup>→ PPT on laptop #2.</sup>
- NO COPY OF MASTER ~~DATA~~ DATA SET

- NO CONVOYS w/ IDS on their process
- [REDACTED] → KNOW NAMES, DON'T KNOW THEIR ROLE IN PROCESS

b6  
b7C

OFF OF LEGAL ADVISOR

→ DISC ~~HS~~ HS ATTORNEY

→ U/S KENNEDY TO CONFIRM DOCS WERE REVIEWED

DELETION/REMOVE

[REDACTED] REMOVED IN.

<sup>CHANCE NOT FOR HIM TO USE FOR "WIPES" & "WIPES" & "WIPES" & "WIPES"</sup>  
b6  
b7C

- SYSTEM THAT WOULD REMOVE/"WIPE" BS/ANDS
- DELETING SO NOT RECOGNIZABLE - DIFFICULT/IMPOSSIBLE TO RECOVER.
- NO SPECIES OF SOFTWARE/PROCESS
- IN JAN 2015 post HOLIDAY.
- NEAR LAPTOP WHILE IT OCCURRED
- ON SPEAKER PHONE w/ HIM WHILE DOING IT.
- DON'T RECALL SELF DELETIONS PRIOR TO PRN.
- " " DISC OF FREE SPACE
- DIDN'T WANT ANYMORE
- ASKED HIM TO REMOVE
- NO NON-PRN CONV. RE. WIPING
- NO RECALL RE "BS/ANDS"

HRC-1772

# PRIOR TO TODAY RETENTION

- DON'T KNOW WHAT IT WAS BEFORE
- " " WHO MADE THE DECISION TO CHANGE
- ON CALL

## DOJ 14

- DON'T WANT TO SPEAK TO B/K DON'T KNOW HOW HE LABIES
- OCCURRED AFTER DOJ PROVIDED TO DOS. CHANGED POLICY TO TODAY'S
- MULTIPLE CAUS DON'T WANT TO SPEC ON A SINGLE TICKET

## JAN 2015 REMOVED FILES FROM COMPUTER

### DELETIONS BEYOND ABOVE?

PRN - NOT AWARE OF

### MARCH 2015 PRN TO DATA CENTER?

- DIDN'T INSTRUCT THEM TO
- AWARE VIA REPRESENTATION

### SEPT 2015 PRN EXPORT / DELETIONS?

- NOT AWARE?
- NO MAINT REQUEST IN SEPT 2015

PRN

### PERSONAL / WORK MIXED CONTENT EMAILS

HA → HC NOT PROVIDED

- HWA HAD EMAILS THAT HC DIDN'T HAVE
- MIXED HC REVIEWED CONTENT TO BEST OF ABILITY.

JAN - MARCH  
→ TIME PERIOD

MECHANICS

### • SORT BY ADDRESS

→ REVIEW FOR WORK RELATED, SUBJECT CASE

### • PUT IN FOLDER AND PRINTED FOLDER (MIXED RECOLLECTION)

• LEFT PERSONAL ONES IN THE BEGINNING

• DIGITAL COPY MADE BY HS.

- SMALLER DATA SETS -

- NOTICED .GUV EXPORT HAD MISSING EMAILS

- ASKED ABOUT ADDITIONAL MISSING DOCS

↓  
TOOK [ ] A COPIE TRIES TO SEND IT.

b6  
b7C

PATTERN OF WHEN A .GUV WAS MISSING. ASKED

[ ] TO PULL (SOMETHING ABOUT WHEN IT  
WAS IN THE .OC LINE)

b6  
b7C

REMOVED BY [ ] IN 2015 w/ OTHER INFO

b6  
b7C

#61

FD-340 (Rev. 4-1

File Number

802

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

74

Date Received

5/28/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A61

MIDYEAR EXAM;  
MISHANDLING OF CLASSIFIED

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

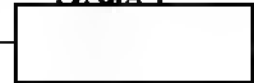
CHERYL MILLS

HRC-1775

5/28/2016 - Cheryl Mills, 8:30A

Pete S.

David I.



b6  
b7C

- After state, personal counsel for Clinton
  - started immediately after
  - Chevy chose for email review @ firm

Alex  
Beth  
Hail

- HS became part of CM firm in 2014
- CM assisted w/ transition to PRN
- ? • Clinton Financial Manager recommended as tech broker



b6  
b7C

- Coordinated needs
- CM doesn't recall requirements, but non-technical focused on experience
- ? • President's office looked at recommendations & selected
- CM negotiated cost & privacy w/ PRN
- CM doesn't know if email transferred
- No knowledge of what happened to Pag. server at time
- No PRN security concerns
- BP served as a reference point / technical translator
- No security concerns about BP server, outsource account
- Did not know about MA laptop @ time & ship in 2014
- Does not know if clintonemail.com email was transferred to hrcoffice.com.
- DM does not believe HRC had access to old email
- CM does not know how HRC accessed



If not on 7th floor, system taped over & even then gone on 7th floor

Summer 2014, State producing last materials for Benhaziz. Dos raised concerns about lack

? [redacted] - meeting with [redacted] email  
[redacted] - not records for HRC & other staff <sup>electronic</sup> b6 b7C

CM suggested searching for Clinton email address

Dos requested seeing [redacted] CM could find email

• Dos contacted CM - phone & meetings

• State - no initial deadline, followed by letter

• CM impression was not that State requesting b/c of FOIA

• HRC asked CM & DK to oversee process, no others

[redacted] State told CM it was HRC obligation to filter out personal. No written doc. b6 b7C

• If sent over .gov, State would not filter.

PRN - [redacted] - CM requested [redacted] provide all email from HRC tenure. b6 b7C

• Jan - March 2009 - HS noticed email missing. CM probably talked to [redacted] about it. [redacted] said PRN did not have. b6 b7C

• Did not reach out for any other providers

• CM does not recall if reached out to AT&T for

Jan-Mar 2009. [redacted] and out at some point AT&T doesn't

• No knowledge of gmail contact [redacted] keep rec b6 b7C

→ No knowledge of other gmail contact

• CM did not communicate w/ HRC on any gmail.

gov  
export

- Apple Server - doesn't recall if tried to access
- Did not request records from others
- Learned of MH laptop after representing
- [ ] provided a remote link - first on later HS. Put file on computer
- No source other than PRN
- No knowledge of where PRN pulled email
- CM requested all gov email from [ ] tenure
- CM doesn't believe PRN was asked or searched HA account.
- "gov" search was to [ ] global (header, text, forwards)
- Late summer 2014 - transfer to CM computer
- [ ] assisted CM remotely. [ ] would send a permission request [ ] then transfer, CM revoke permission
- Doesn't know where saved or if encrypted. Were password protected
- No copies of .gov. or transferred to other media
- Imported into outlook
- Did not consider any ediscovery tools
- Dell work laptop, some personal use
  - in CM's attorney's possession
  - no other computers
- connected to internet yes antivirus
- not wiped or reset, continued to use

b6  
b7C

b6  
b7C

- Dell still in use when turned over

- CM never rec'd DVDs. Discussed DVDs, but  recommended secure remote transfer

b6  
b7C

3 • CM <sup>July 28</sup> does not recall conference call - archived email options

- Does not recall any other conversations w/  about gov.

b6  
b7C

- HS conducted reviews - doesn't know process HS   
• ~~separate gov.~~ using at that time

- CM requested full export in fall (CM doesn't believe gov review complete)

- Requested full archive to review any non gov work related

- Doesn't know mailboxes, etc. searched

Full archive CM requested all email from tenure (Jan 21, 2009 - 2/1/13)

- CM did not instruct PRN to search HT email

- CM doesn't know email addresses

- PRN used remote transfer to HS.

- CM doesn't recall if ~~status~~ transferred to her

- PRN only went back to 3/18/2009

- CM doesn't know what effort to recover 1/2009-3/2009, but outcome - unavailable.

- CM rec'd no other transfers, HS smaller transfers when HS identified gaps

- Only conv. CM recalls about gaps was 1/09-3/09

- CM does not know of a look master copy

- CM never had direct access to mailbox

- HS only one reviewing full set

## • Process

- filter .gov
- key words
- senders
- Review took several months. Took place @ Mills' office
- HS used her computer
- HS would sometimes ask CM for guidance
- Email printed after review
- Made copy & gave to WGC
- CM did not review 30k
- Might have been duplicates - not sure
- Not involved in attempt to de-duplicate
- Collectively developed process
- Doesn't know why work related between HA & ~~HA~~ email.com not in what produced to State
- Not aware of any distinction between treatment of HA state.gov & HA ~~clinton~~ email.com
- No consultation w/ non-agents
- Mixed use treated as w/ related
- Not aware of any efforts to de-dup
- HS review took months
- Docs turned over [redacted] Dec 2014
- Emails w/ [redacted]
- PRN explained email would display as whatever current mail <sup>of concern</sup>
- Nothing removed w/c classified or sensitive

- No memory of HS needing to have connection re-established

Don't recall 11/24/2014 urgent call w/ PRN

press

not on all calls w/ PRN. HS would sometimes talk directly to PRN.

- Records turned over Dec 2014
- No separate review after ~~the~~ HS complete
- After review, official copy of pst given to DK + HS kept working copy on computer. CM does not know who produced or what named. only recall request from OF 1. gov + delete.
- Remote session on 1/2015 w/ [ ] - he removed & looked around for any other files. Link-permission-acknowledged & deleted w/ program - revoke permission. More than recycle bin. Looked w/ [ ] to verify. Does not know which program. b6  
b7C
- May have discussed wiping software w/ BP. no memory
- No non-agent - wiping
- Don't know what BlackBit is or what PRN used.
- After [ ] added she didn't want to retain email, [ ] to 30-60 day retention policy & did not need any historical. b6  
b7C
- CM did not instruct to remove exported pst or archive mailboxes
- Around 1/5/2015 was when [ ] removed files from computer. Only [ ] - no others
- Not aware of any deletions in 3/2015 by PRN

Dec 2014  
Jan 2015

- 2015 - Instructed PRN to visit datacenter
- reviewing old systems from 2013 - that were Clinton's
- wanted to confirm no other records on old equip.
- PRN could not locate anything on old systems
- Told PRN to maintain equip.
- Sent document retention to PRN in 3/2015
- Did not request HRC Archive deleted in 3/2015
- No instruction to delete any other pst
- No inst. to delete Datto.
- No inst. to delete pst w/ Bleach Bit on 8/31/2015.
- No request to create additional exports in 9/2015

- 
- No discussion of potentially classified
  - Direction from state after production to delete classified (retro)

#63

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-302

b3  
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

78

Date Received

6/10/16

From

JOHN BENTEL

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A63

MIDYEAR EXAM

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

JOHN BENTEL

REFERENCED DOCUMENTS

HRC-1789

~~Phisher?~~

John Bentell

JB DAS tenure - 39 yrs.

Always exec sec

Director of S/ES 08 - '12

Lew Lewkins

Trule Mus

— Supervisors

IRM  
POEMS

80-85

under JB

2 deputies

~~Phisher?~~

Server - learned when it came out in paper.

had no knowledge of personal server during tenure.

b6  
b7C

1st EMAIL - "Sec Res. Installation Hotwash"

don't remember email

[redacted] secure comms / phones @ Front office & residence

b6  
b7C

[redacted] - Contractor in [redacted] Section.

"Hotwash" - Summary of equipment installed by DAS in HRCs home.

ref. to server in basement closet" - Not sure

what it would have been in ref. to.

Under JB but not the specific

sent to JB b/c of position: likely a collective

not sure would have looked @ the email.

→ in detail.

2nd email 2yrs later after Irene. / don't recall email.

"I wouldn't have used term Chap Server"

Don't recall <sup>HRC</sup> losing connectivity during Irene.

or conversations re: connectivity [Monica Hanley]

don't recall any conversations re: email outages.

HRC-1790



also talked to

[redacted]

Team

Teen Team

JB

didn't get a lot of direct calls  
from 7th floor.

Not HA or CM.

Re: OIG report.

still w/ DOS. don't recall conversations

Not style - wouldn't have responded that way.

would have tried to settle it wouldn't have  
shut down.

Didn't talk w/ anyone @ DOS re: server.

S/ES IRM - no know of setup of server

Met Bryan Pag - not sure when / casual.

Wanted for "BIG IRM" - maybe mobile comm. division

- no knowledge of support on side.

EMAIL

"don't remember when I learned"

knew she had a personal email

didn't know using personal email for DOS business

don't remember if HRC had a DOS email  
account.

Help desk handled.  
Never aware of issues being reported about sec/  
personal email.

~~4/20/2011~~

haven't spoken to anyone @ Das. to matter since learning.

Aug 30, 2011

Email 3 - don't recall, but a/c. write email during Har Irene.

email address - systems admin likely set up.  
don't know why previously set up.

FOIA remark - "Just when you have a Das device  
it was subj to FOIA" - "Just wanted her to know!"  
If using for personal messages - subj to FOIA

RMD - not responsibility:

don't recall ever discussing FOIA w/

maybe staff wise

b6  
b7c

SMART - somewhat familiar: <sup>function to</sup> decide what is/isn't a record.  
not used by POEMS S/ES IRM - not opposed  
getting things out. Didn't want to implement  
until fixed Exec Sec / Mail would have decided on rollout  
~~then~~

I just don't remember that @ all. [Re: server]

**From:** Lee, Purcell N  
**Sent:** Tuesday, March 17, 2009 1:35 PM  
**To:** Wagganer, Kevin L; Bentel, John A; Scott, Andrew C  
**Cc:** Duncan, Bruce E  
**Subject:** Secretary Residential Installation Hotwash  
**Attachments:** Secretary Residential Installation Hotwash.docx

Attached is the agenda/talking points for the hot wash.

## Secretary Residential Installation Hotwash

### 1. Equipment location:

- a. Unclassified Partner System:
  - i. Server: Basement Telephone Closet
  - ii. Telephone Set: Various rooms
- b. Classified Red Switch: Third Floor
- c. Classified Red Switch: Third Floor

### 2. Status of Installation:

- a. Unclassified Partner Telephone System: Completed.
- b. Classified STE/Fax: Completed
- c. Classified Red Switch: Completed
- d. Unclassified Ops Drop: Verizon is still working to finalize path.
- e. CMS Classified Video: Declined
- f. CMS Classified Voice: Declined

### 3. Issues:

- a. T1 Telephone Services were not available upon arrival
- b. Analog lines (2) for the Partner system was not ordered.
- c. Red Switch Technicians arrived 2 days later than scheduled.
- d. SDS Data Cable was left in Washington
- e. Former President's wireless headset was disconnected
- f. Secretary Clinton's headset noise cancelling was not selected
- g. Speed Dial for Secretary Clinton Unclassified telephone was not working properly.
- h. Secretary Clinton's business lines were not set up in a "Hunt Group"

**From:** "Hanley, Monica R" <SBUSTATE/SES/RECIPIENTS/HANLEYMR>  
**Sent:** 8/30/2011 5:32:36 PM +00:00  
**To:** 'huma@clintonemail.com'; "Abedin, Huma" <AbedinH@state.gov>  
**Subject:** HRC blackberry

John bental (202-647-4656) just called me abt getting hrc a new blackberry for the paris trip. He said that he heard that the chapp server is down. He said that the she spoke to the comm guy directly abt it this morning.

It looks like she's receiving email on her ipad. Does she want a state berry for the trip? They wld like to know this afternoon so that they can set up.

I told him that I wasn't sure and that I wd ask you.

PR\_RIM\_INTERNET\_MESS [REDACTED]  
AGE\_ID: .state.sbu>  
PR\_RIM\_PAGER\_TX\_FLAG: true

PR\_RIM\_MSG\_STATUS: 1  
PR\_RIM\_MSG\_ON\_DEVICE true  
\_3\_6:  
PR\_RIM\_MSG\_REF\_ID: -1561860114  
PR\_RIM\_MSG\_FOLDER\_ID: -6

b6 Per  
b7E DOS

PR\_RIM\_MESSAGE\_SUBMISSION\_ID: [REDACTED]

---

**From:** "Hanley, Monica R" <SBUSTATE/SES/RECIPIENTS/HANLEYMR>  
**Sent:** 8/30/2011 10:09:28 PM +00:00  
**To:** "Abedin, Huma" <AbedinH@state.gov>  
**Subject:** Re: S berry

Do you want a different address?

----- Original Message -----

**From:** Abedin, Huma  
**Sent:** Tuesday, August 30, 2011 05:19 PM  
**To:** Hanley, Monica R  
**Subject:** Re: S berry

That can't be it.

----- Original Message -----

**From:** Hanley, Monica R  
**Sent:** Tuesday, August 30, 2011 04:19 PM  
**To:** Abedin, Huma  
**Subject:** Fw: S berry

SSHRC@state.gov

----- Original Message -----

**From:** Bentel, John A  
**Sent:** Tuesday, August 30, 2011 04:15 PM  
**To:** Hanley, Monica R  
**Subject:** RE: S berry

Monica: We actually have an account previously set up: SSHRC@state.gov. There are some old emails but none since Jan '11 -- we could get rid of them.  
You should be aware that any email would go through the Department's infrastructure and subject to FOIA searches.

Let me know if any questions and what you would like us to do.

Thanks!  
John

SBU  
This email is UNCLASSIFIED

-----Original Message-----

**From:** Hanley, Monica R  
**Sent:** Tuesday, August 30, 2011 3:59 PM  
**To:** Bentel, John A  
**Subject:** S berry

Do you know what her email address would be on a state dept berry?

---

PR\_RIM\_INTERNET\_MESS

AGE\_ID: state.sbu>

PR\_RIM\_PAGER\_TX\_FLAG: true

PR\_RIM\_MSG\_STATUS: 1

b6 Per  
b7E DOS

HRC-1796

PR\_RIM\_MSG\_ON\_DEVICE true

\_3\_6:

PR\_RIM\_MSG\_REF\_ID: -1805720130

PR\_RIM\_MSG\_FOLDER\_ID: -6

PR\_RIM\_MESSAGE\_SUBMISSION\_ID:

b6 Per  
b7E DOS



*Partner*

b6  
b7C







b6  
b7C

ABU DHABI AUSTIN BEIJING BRUSSELS DALLAS DUBAI HONG KONG HOUSTON  
LONDON MOSCOW NEW YORK PALO ALTO RIO DE JANEIRO RIYADH WASHINGTON

FD-340 (Rev. 4-1)

File Number

302

Field Office Acquiring Evidence

WF

Serial # of Originating Document

91

Date Received

6/6/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

To Be Returned

☐ Yes

☒ No

Receipt

☐ Yes

☒ No

Grand Juror - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A75

MID YEAR EXAM;

MISHANDLING OF CLASSIFIED

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

and documents  
provided by

6/6/2016

3/5

b6  
b7C

Commercial / Open Source - No USG info systems  
used to create

Works for

(Defense Contractor)

b6  
b7C

• Missile Space Air Force + Intel

Owns

b6  
b7C

• focuses on all domestic data

b6  
b7C  
b7E

records

b6  
b7C

• DHD - Dark Horse Data, Inc ← Reginald Hyde (owns)  
four DASDI ←

- Works w/ foreign data
- Can contract w/ govt
- embed w/ client

Project

b6  
b7C

June 2015 - [redacted]

[redacted]

[redacted] Sr. Staff on senate judiciary comm.

June/July 2015

[redacted] concerned w/ email server data ending up overseas

b6  
b7C

- Was it hacked? If so, OCONUS? If OCONUS, foreign power?
- Three sons marines, worried would endanger
- Upset as staff & citizen

[redacted] asked [redacted] how to figure out

b6  
b7C

[redacted] said need known data

[redacted] asked [redacted] what end product/state

looking for genuine, authentic, relevant

from HRC server

not altered

from HRC server

move OCONUS place where foreign actor could access?

• Not yet being paid.

Aug/Sep. 2015

[redacted] goes to Newt Gingrich for guidance

b6  
b7C

[redacted] meet w/ NG [redacted] briefs potential project

- All three bothered by potential data was comp.
- NG wanted to talk w/others

b6  
b7C

[redacted] pitched to several organizations (needed funding)

Dec 2015 • NG tells [redacted] to meet w/ [redacted] (Judicial Watch)

- Phase 1 was HRC server directly or ind. attacked?
- Phase 2 "SB"
- Phase 3 was data moved outside of 4 walls
- Phase 4 exposed to foreign service

[ ] said if he thought data classified, would have to report

b6  
b7C

- Discussed what to do if found classified

[ ] discussed

b6  
b7C

• Then moved to law firm [ ] Watch.

Jay/Feb  
2016

- Firm's view was couldn't be [ ] but to  
via open source, no obligation

(following 4th)

- Funding/pace of Judicial Watch actions not  
paced around election

- 3 funding streams: contractor (self-funded,  
gov't funds, or data arbitrager)

- Funders invest in litigation on prospect of judge awarding  
fees at end. (gov't would have to pay fees)

- Phase 1 - \$32k from Judicial Watch to [ ]

b6  
b7C

- [ ] was b/c JW confident he understood data, dark  
web, etc.

on original work-papers & agreed orally

- [ ] had one condition - if found classified,  
would turn over fruits of project, even given  
att.-client priv.

- Ended in March 2016

Feb 2016  
[ ]  
raise on  
reider threat

→ - Where to get data?

Feb/March  
2016

- HRC + SB email accts on [ ]'s

- Offshore servers off limits

- Sidebar - company wanted to index deep/dark-web

- intake entire deep/dark web onto own servers + index

- company could be good solution to problem

[ ] is name of company

b6  
b7C

[redacted]  
Their data allowed [redacted] to go into deep/dark web w/o going to Guccifer ~~but~~ servers.

[redacted] asked [redacted] to do search [redacted]

- Principal had left in 12/2015

[redacted] asked [redacted] to find indication under 4pt. plan

[redacted] gave [redacted] check for \$2500

[redacted] gave [redacted] back a schematic. *obtained from email; proofed by JW.*

[redacted] created search logic/code (HRC, IP address, blumenthal domain..)

[redacted] believed SB had physical server

[redacted] doesn't look @ webmail

- only attachments, no email in deep/dark web
- Believes was back of workstation b/c no email
- Files land on server in Romania

→ meet four point criteria

84.232.210.154 - some say Guccifer server

~~others~~ co-conspirator

- others foreign service

• Word, Excel docs among 200 files

- some appear to be his wife's

- look @ titles

[redacted] believed

b6  
b7c

- Blamethat server hit multiple times
- 5/22/2009 hack of server - could not recall - possibly from public report. Looked & cannot find source
  - Did not find evidence of intrusion to HRC server in docs reviewed.

- Very sensitive - targeting data
  - did not come from SB server
  - contained IP block range that incl. Clinton server
  - link leading to document
  - names of known/suspected jihadists in Libya
  - lower portion of document in Russian
  - Excel

- After ~~reviewing~~ document project stopped

- Jan <sup>20th</sup> 2012 - Person can [redacted] to [redacted]
  - compare to SB dates

b6  
b7c

- Rogue nation judgment recovery program
  - [redacted] Naturalized USCit [redacted]

- 2013/4 meets w Tyler Drumheller
  - wanted to stand up program
  - contract w/ opposition gov't. - access to Libyan central bank data

Phase 1 complete - about to deliver final product

Would pull down 371c.

• Talk w/ [redacted] re: rogue nation.

• Libyan FM.

• Only used [redacted] data

• Likely will remove 5/22/2009 reference





Notes

b6  
b7C

PREPARED BY [redacted]  
DATE 06/06/16

[redacted] Interview 10:00AM - 12:30PM  
Washington Field office

b6  
b7C

PROJECT ACTION NOTES

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
PROJECT DATE 12-01-2016 BY J76J18T8D NSICG

[redacted]

b6  
b7C

6 All material is his opinion, not USG;  
7 no USG databases used/accessed  
8  
9 Three hats: <sup>data#</sup> [redacted] vice of [redacted]  
10 [redacted] (space, air force,  
11 defense, intel) - direct military contractor

b6  
b7C

12 Hat #2 owns [redacted]  
13 does no investigation, focuses on data -  
14 domestic acquisition. [redacted]

data fusion

15 [redacted]  
16 [redacted]  
17 [redacted]  
18 [redacted]  
19 [redacted]  
20 [redacted]  
21 [redacted]  
22 [redacted]

23 [redacted] talked  
24 to each other & created one of  
25 largest databases out there.

b6  
b7C

26  
27 Background in [redacted]

b6  
b7C

28 [redacted] HRC-1808

PREPARED BY

DATE

PROJECT ACTION NOTES

PROJECT PLANNING NOTES

Hatt ③ DHD - Dark Horse Data, Inc

- [redacted] owned by Reginald Hilde b6 b7C

(former DAS DNI)

- Adv. proving tech. as it relates to data, mainly does/focuses on foreign data. b6 b7C

- [redacted] does not contract with govt. (USG)

- DHD works directly within USG agencies as contractors



b6  
b7C

Around 6/2015, woman by name of



b6  
b7C

[redacted] approached [redacted] because

she's concerned about [redacted] email server.

Concern is two pronged: foreign govt acquisition of data / risk to US, general concern as an USPER.

- Poses question: is there a way to figure out if the concerns ~~are~~ can be proven (loss of data, etc.)

- objective: ← Was it acquired / available to foreign intel

- Research would be open source, Deep / Dark Web

HRC-1809

Sr. staff member on Sen. Judiciary Committee

Data:

- Genuine  
Did it come from where it purports?

- Authentic  
Is it real?

Relevant:

- Did it come from [redacted] server, was it [redacted] did it reside in [redacted]

moved offshore, place a for. govt. had access to it?

## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

Aug/Sept  
2015

- 1 [redacted] was convinced there would be b6  
2 people interested in this. b7C
  - 3 [redacted] asks Newt Gingrich for advice
  - 4 on whether to execute the plan for the
  - 5 project.
  - 6 - Gingrich, [redacted] all b6  
7 "revised" by the server event b7C
  - 8 - Approached companies for funding/interest
  - 9 but [redacted] not impressed by them.
  - 10 - Around Dec. 2015, Gingrich b6  
11 says to go see [redacted] (sp?) [redacted] b7C
  - 12 of Judicial Watch.
  - 13 - [redacted] lays out Phase I plan to [redacted]
  - 14 ① was Clinton's server attacked
  - 15 ② was Blumenthal's server attacked
  - 16 ③ was the data stored outside the U.S.
  - 17 ④ was data exposed to for. service
  - 18 - The 'what if we find classified info'
  - 19 came into play ← concern of [redacted]
  - 20 [redacted] b6  
21 [redacted] b7C
  - 22 - law firm for Judicial Watch
  - 23 states info has to come from
  - 24 open source, no hacking
  - 25 allowed, and data acq. had
  - 26 to follow four-point plan/criteria
  - 27 - No real answer from law firm
  - 28 about what happens if classified
- HRC-1810

## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

Data  
Projects

1. [redacted] adds Judicial Watch's motivation  
 2. was no political (i.e. related to the elections)  
 3. but it was more of a longer-term interest

1. Self-funded - you assume risk
2. Govt funded - govt assumes all risk
3. Data arbitrageurs - invest \$, like seed money

Judicial Watch goes to funders, and  
 states project will yield returns if  
 J.W. wins litigation with State Dept.  
 - This is the reason J.W.'s agenda  
 is not political

Phase I: \$32000 from J.W. to [redacted] b6 b7C

[redacted] believes he w<sup>s</sup> selected over others  
 because of his familiarity with data  
 (running things from inception to end)

- caveat [redacted] adds: if data he  
 comes upon is deemed classified, b6 b7C

the data would be turned in  
 to the authorities

- Feb/March 2014 ~ project is funded
- Where are you going to get the data  
 without hitting the server? HRC-1811

- solution: [redacted]

[redacted] thinks

This could be the solution

b6  
b7C

Included in  
 the original  
 work papers. If  
 it wasn't, it was  
 clearly relayed/  
 agreed upon  
 orally.

brought in to

Feb. 2012 or 2011  
PROJECT ACTION NOTES

to index the Deep/Dark web. (2009 timef.)

— company name is [redacted] which  
had a commercial & govt. services

b6  
b7C

— for [redacted] attractive because it  
allowed him to query the data w/o  
hitting any servers — anonymizers  
were too much a risk

b6  
b7C

— went to [redacted] and  
asked to conduct a query in Dec. 2015  
but guy was no longer available  
when the funding became available

because [redacted]

leaves comp.  
in Dec.

o might've had to do with the  
business model the company  
was running.

b6  
b7C

explained to [redacted] by  
the same guy he had approached  
in Dec. 2015.

— [redacted] needed an indication,  
based on specific data queries,  
that data had originated from  
the Clinton server.

b6  
b7Cb6  
b7C

— [redacted] returned a schematic

## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

- ①
- two spreadsheets: chron order data is first seen w/ yellow highlights that hit on the query logic
  - yellow = hit on keywords

keyword  
search:

obtained from  
email header  
(from J.W.)

hrc, Blumenthal, Libya, clintonemail.com,  
IP address of Clinton server, and  
→ possibly Blumenthal's server IP.

- [ ] believes Blumenthal did have a server, and that's how the data spilled (meets data project criteria #1)
- Blumenthal clicks on a link/attach. #2

and comp. content is exfiltrated.

Substantiation is the fact that only documents, not emails (pst files) are found by [ ]

b6  
b7c

- Data resides in server over which meets criteria #3

- ②
- second spreadsheet: belief this is the Russian anonymous server
  - opinion that it isn't Guccifer's server. It's someone else.

## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

1 - of 200+ Sidney docs, other than the  
2 memos, there are word and excel docs.  
3 keyword search: diff. family  
4 members, etc. "ctrl+F: blu"  
5 infers this number based on filenames.

7 - Hacking Blumenthal server more than  
8 once (Guccifer)

9 - Based on the fact that the data  
10 is first seen on different dates  
11

12 - May 22, 2009 penetration of Clinton server

13 - Not sure about where this came  
14 from, but prob. an open source.

"It was told to  
me"

- probably  
from [redacted]

16 - In assessing memos' tone, Blumenthal  
17 amped up the data provided to him by b6  
18 sources and Drumheller. b7c

20 - of the 200+ [redacted] only got/read b6  
21 the ~20 memos b7c

23 - The "smoking gun" doc: it did not  
24 come from the Blumenthal server  
25 but the doc - email with a block  
26 that went <sup>to link</sup> back to the Clinton  
27 server.



## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

"smoking gun document":

— purported names of terrorists/  
jihadists in Libya. (per filename)

— Names not checked

— lower/bottom half contains  
Russian/Cyrillic script.

— scenario: doc goes from hand  
to hand and spills.

b6

b7C

Not approved yet

Phase II has been presented

"Look very  
carefully into  
this guy's  
background"

Guy came to [redacted] in Jan. 2012 (maybe  
Jan. 20, 2012)  
which [redacted] is the date the Blumenthal  
memos

[redacted] claims he was hired by the  
Libyan opposition govt. Judgment

b6

b7C

— Libyan Rogue National Recovery  
program

b6

b7C

For recovery of  
Gaddafi assets

[redacted] & Drumheller & [redacted]  
[redacted] probably all knew  
each other

Questions whether  
Blumenthal was  
involved

[redacted] met Drumheller, who  
was involved in the Recovery  
Program

b6

b7C

— The customer was the opposition  
govt.

HRC-1815

## PROJECT ACTION NOTES

## PROJECT PLANNING NOTES

1 - Blumenthal, if involved in the Recovery  
2 program, wrote memos as a "shake  
3 and bake" tactic.  
4

5 - Has not done any Deep/Dark web  
6 research of his own - too risky  
7

8 - Might pull the May 22, 2009 statement  
9 out of the final report.  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

HRC-1816

Jul 9

### 3 June Meeting – Proposed Agenda

Here is a proposed agenda, but I defer to the host to change or delete any portion that it feels is unnecessary or inappropriate

#### Introduction and Background

- Background of the Principals,
- Caveats –Not a USG Project; no systems, sources, methods, means, personnel, data, or any other resources of the USG were employed, only commercial off the shelf resources, both known and unknown to the principals.
- Background of Project as authorized by customer JW.
- The Phase I Scope and Order of Magnitude

b6  
b7c

#### I. Results of Phase I – Was SB server or computer entered and if so, did the data move offshore?

1. SB Server was entered directly and data was moved to Guccifer server or computer.
2. SB server contents was then moved from Guccifer server to a second IP nearby.
3. Not clear who this second server is owned by, but data was definitely moved.
4. Data includes memos from SB to HRC and found on SB server.
5. The secondary source has over 37,000 files on it, and many (over 200) trace to SB. Of these, 25 or so were traced and recovered, all of which show positive indications as having been authored by SB, sent to HRC, and recovered.
6. The discussion within these memos suggest SITREPs and alleged Intel Assessments using HUMINT on the ground in Libya.

#### II. Results of Phase II – Was HRC attacked directly or indirectly?

1. Of the 37,000 files, we would need to open each and trace back the content to the original server. The Phase I assignment did not include a scope of this magnitude.
2. However, Key word searching of the spreadsheet show many references to HRC and other symbols that may be files that came directly from the HRC server. It is unknown at this time whether there was a direct, pernicious attack and wholesale exfiltration, based upon the evidence assembled to date.
3. One file was recovered but the providence is not clear. This file has attributes that are similar to other Libyan-based SITREPS, that were found. The time, topic, context, names, and background all seem to align with these suspected attacks. However, much additional research is needed to trace this document to its original source.
4. The document did not come from SB or was not found among files that came from his computer. It did bare, according to one source, signatures of the IP for the HRC server

and is suspected to have come from her computer or at least a computer linked to an IP address that ties to where the server was in 2009.

If this document is deemed to be genuine, authentic and relevant to the issues here, it represents a major loss of grave concerns.

### **III. Results of Phase I – What was the possible motive of SB? Was it to create a quid pro qua?**

1. Rogue National Judgment Recovery Work.
2. Work with the Libyan Opposition Government
3. Work with the new foreign minister as a back channel

### **IV. Way Forward**

1. A number of possible ways to obtain more specific evidence as to SB motive and to check the veracity of the Rogue National Recovery Program connection to SB and others.
2. Recover all 37,000 files under the International Bulk Data Silo Procurement Program. Could be done by the host, or could be contracted or could be part of Phase II. Many different options on where, how and when to collect the data and subject to analysis.
3. Check the provenance of the key document and try to trace it back to the original source.

### **Questions or Comments**

in:sent

UPK 9

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-01-2016 BY J76J18T80 NSICG

Move to Inbox

Gmail

COMPOSE

Phone call

Inbox x

Inbox

Starred

Important

Sent Mail

Drafts

Circles

Deleted Messages

Notes

Personal

Saved

Travel

More

[redacted]

[redacted]

Please send as we discussed. Thank you and look forward to meeting yo

b6  
b7C

[redacted]

Hey [redacted]

I couldn't download the file via the link sent in a separate email...

b6  
b7C

[redacted]

Thanks - I was able to download all the files. On Thu, Jun 2, 2016 at 10:17 A...

b6  
b7C

[redacted]

to [redacted]

[redacted]

b6  
b7C

A somewhat urgent update:

For the past six weeks when the hypothesis of the SB portion of the report was over the dates of the seminal events, the key name of the person, and the com with any evidence tending to support the timeline.

I finally recalled the way to track this down much to my relief because for a whi recollections on this issue and confusing facts. Indeed, I was not. Below are s lines as a means to determine whether the hypothesis has any merit at all.

Sign in

Signing in will sign you into  
Hangouts across Google  
Learn more

Friday, January 20, 2012 1145 AM

Email to [redacted]

Friday, January 20, 2012 1150 AM

EMAIL TO [redacted]

Monday, January 16, 2012 1015 AM

EMAIL TO [redacted]

Monday, January 16, 2012 1015 AM ver2

Saturday, January 07, 2012 1103 AM From [redacted]

AOL

Thursday, January 26, 2012 1111 AM

EMAIL TO [redacted]

b6  
b7C

If you wish, I can update the draft memo to reflect context of this over the week have discovered.

Revert to the old chat

I will highlight the relevant section in Yellow so that it fits the story line and conl

Let me know if this is something you wish, or if you just want an oral brief as a should be done at some point, only because it is really important data and has have been mystified about since I was engaged on this matter.

Take me to Inbox

HRC-1819

6/6/2016 7:29 AM

**EXECUTIVE SUMMARY OF RESEARCH FINDINGS**

In addition to the above, the Phase I Study resulted in some other detailed findings that are best summarized below:

1. The computer of Sidney Blumenthal was positively identified as hosting many emails and attachments originating from Hillary Clinton's server and others from the Clinton Foundation. In Phase I, we recovered at least 20 memos from Mr. Blumenthal to Mrs. Clinton that contained Situation Reports (SITREPS) allegedly based upon intelligence sources in Libya.
2. Mr. Blumenthal's server was successfully attacked by Marcel Lazar Lehel, originally from Bucharest, who is also known as *Guccifer* or "Small Fume".
3. While one spreadsheet shows that over 37,000 files were found on a closed encrypted and password protected site of someone other than *Guccifer*, only a full analysis of the spreadsheet will reveal all of the files traced back to Mrs. Clinton's server directly, or to that of Mr. Blumenthal. These files were traced to a computer that was using an application to access the Peer-to-Peer networks. The computer was traced to IP address 84.232.210.154, which points to Bucharest, Romania.
4. One search revealed that data that originated from Mr. Blumenthal's server was transferred to the computer at 84.232.210.154 on July 5<sup>th</sup> 2014 at 07:12 (Bucharest Time), and yielded many references to "HRC" within the spreadsheet. This would suggest that the content of the computer traced to IP 84.232.210.154, was not *Guccifer*, but someone else who accessed his server. The reason is that this "migration" occurred long after *Guccifer* was identified, arrested, and incarcerated in Romania. Several possible explanations exist:
  - (a) *Guccifer* had a co-conspirator that continued to operate the collection from various sources as a "get out of jail free card";
  - (b) The computer doing this collecting did belong to *Guccifer*, and he allowed it to run long after he was arrested. This scenario seems unlikely for a number of technical reasons.
  - (c) This computer belongs to a foreign service or someone else who attacked the *Guccifer* server and transferred the data to computer 84.232.210.154.
5. Notwithstanding the above, data from both the Blumenthal computer and the Clinton email server migrated to *Guccifer*, and then to a computer tied to IP 84.232.210.154, both of which were located outside of the United States and outside of the control of the US Intelligence Community. Assuming

either contained overtly classified data or retrospectively classified data, this is considered a major Counterintelligence concern and of interest to the Community.

6. *Guccifer* entered the Blumenthal computer several times, first through Blumenthal's AOL account. It is not clear whether *Guccifer* targeted Blumenthal because he represented an opportunity of interest, or because a foreign service directed him to the account. Also, it is not clear whether the account was entered after he first entered the Clinton server or that of someone else on the Clinton domain server.
7. During Phase II, much additional information can be obtained on the sequence, timing and chronology of when the two servers in question were accessed and in what order and how many times.
8. We found indications that *Guccifer* or person or persons acting on his behalf or persons impersonating *Guccifer* did a secondary penetration of Mrs. Clinton's server on May 22, 2009, and other penetrations thereafter.
9. We confirmed that *Guccifer* used an anonymous server located in Russia to conduct the penetration, and therefore, there is a high possibility that the Russian services that monitor these anonymous servers likewise have a copy.
10. One file that was found on Mrs. Clinton's server was not found on the Blumenthal server. This file represents a major loss to the Intelligence Community because it appears to be targeting data. The data is first in Russian and then converted to Arabic. It represents a list of targets that quite possibly was created by a Russian source, located or intercepted by our services, and transmitted to Mrs. Clinton by some unknown person. The file then left her server and was found in the Deep Web and Dark Web.
11. The above cited file, an excel spreadsheet, we assess, would enjoy the highest level of classification if submitted to a person who has original classification authority. The file was found stripped of its collars (if they ever existed). If it is determined by the FBI that this file ever was overtly classified, it will serve as a potential "smoking gun document."
12. *Guccifer* penetrated a number of targets and we recovered over 37,000 files from a computer traced to IP 84.232.210.154 that he obtained. We created a mapping of those files as they appear in the Deep Web. We then tested the spreadsheet and the content behind the spreadsheet (the 37,000 files) using key word fuzzy logic. We confirmed the following Blumenthal memos were found on the Clinton Server and vice versa:

Name	Date Rec'd	File Name	File
84.232.210.154\hrc_memo_algeria Libya 021112	7/5/2014 7:12 AM	Microsoft Word Document	13 KB
84.232.210.154\hrc_memo_algeria Libya 031012	7/5/2014 7:12 AM	Microsoft Word Document	13 KB
84.232.210.154\hrc_memo Comprehensive Intel Report on Libya 010312	7/5/2014 7:12 AM	Microsoft Word Document	21 KB
84.232.210.154\hrc_memo Comprehensive Intel Report on Libya 010412	7/5/2014 7:12 AM	Microsoft Word Document	21 KB
84.232.210.154\hrc_memo Libya fear & thinking 080912	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\hrc_memo Georgia US elections flashback 090212	7/5/2014 7:12 AM	Microsoft Word Document	26 KB
84.232.210.154\hrc_memo intel berke marx & opposition 120812	7/5/2014 7:12 AM	Microsoft Word Document	17 KB
84.232.210.154\hrc_memo Latest French Intelligence Reports on Al Qaeda Hostage Crisis 011012	7/5/2014 7:12 AM	Microsoft Word Document	10 KB
84.232.210.154\hrc_memo Libya Benghazi on 101013	7/5/2014 7:12 AM	Microsoft Word Document	18 KB
84.232.210.154\hrc_memo Libya cabinet 100612	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\hrc_memo Libya internal gov 011512	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\hrc_memo Libya new president 080712	7/5/2014 7:12 AM	Microsoft Word Document	19 KB
84.232.210.154\hrc_memo Libyan Leadership Private Discussions 102512	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\hrc_memo maganef attack on US in Libya 091212	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\hrc_memo Merkel German eco Intel 090412	7/5/2014 7:12 AM	Microsoft Word Document	27 KB
84.232.210.154\hrc_memo more maganef private reass 091312	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\hrc_memo more maganef 091412	7/5/2014 7:12 AM	Microsoft Word Document	18 KB
84.232.210.154\hrc_memo more maganef's private conversations 091412	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\hrc_memo patraux october surprise 111012	7/5/2014 7:12 AM	Microsoft Word Document	12 KB
84.232.210.154\hrc_memo patraux october surprise 111212	7/5/2014 7:12 AM	Microsoft Word Document	12 KB
84.232.210.154\hrc_memo turkey us synops plus intel 100312	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\hrc_memo Egypt north how 031313	7/5/2014 7:12 AM	Microsoft Word Document	17 KB

13. A complete copy of the Blumenthal memos sent to Mrs. Clinton were opened recovered in original format and deserves critical analysis by counsel. Most all were word documents and related to a number of issues. These can be provided to counsel as a means to substantiate the claims of Guccifer.

14. We did not actually collect the content of Mrs. Clinton's server or the content of computer 84.232.210.154 at Phase I; we merely validated the major premise and hypothesis that data originating from either or both of the Clinton and Blumenthal servers were attacked, directly or indirectly, and then were moved outside of the US to Guccifer; and then migrated to computer IP 84.232.210.154, owned and operated by unknown persons. Additional research is required to cull through the 37,000 files found to select those that pertain to Mrs. Clinton and which came directly from her server.

15. We note that there are profound legal questions regarding Phase II because it is not clear what our obligations may be regarding recovery of potentially classified data that may or may not contain actual collars that overtly show the content was classified at the time they were sent to Mrs. Clinton; or emails and attachments that were retrospectively classified but were released in truncated form. Our recovery of such content would be untruncated and in original condition.

16. It is conceivable that one possible motive for Mr. Blumenthal's decision to feed Mrs. Clinton the SITREP reports was to promote his group as a quality private intelligence group in Libya capable of obtaining detailed intelligence from various unnamed, disparate sources as to the thinking, actions, planning and intentions of key operators in the region. We do not opine on



the accuracy of the intelligence provided, only the tone and intent of the memos. Our assessment is that they are essentially, crafted as "shake and bake" intelligence assessments, done to promote a need by the Blumenthal group, and not to turnover information because of some legal or moral obligation.

17. There is objective evidence to indicate that a person identified as [redacted] telephone [redacted] (circa. 10 January 2012) began to solicit Senior Intelligence Analysts with experience in repatriation of assets plundered by the Qaddafi family. This person began the solicitation process on approximately January 25<sup>th</sup> 2012, claiming that he led was dealing with representatives of a "high level political types in the US within the State Department" and that he personally had high level contacts within the new Libyan Opposition Government that he would have a contract with to begin the repatriation process.
18. [redacted] has a rather controversial history within the US Intelligence Community, particularly at [redacted] His links to [redacted] was one of the prime operatives in Libya. Notwithstanding his reputation in the US Intelligence Community, he was believed to have highly placed contacts within Libya which could have been mined for creation of a Rogue Nation Asset Recovery program, but for his limited technical and intelligence analyst resources.

## Phase II

The proposed Phase II study includes:

1. Recovery and sorting of all *Guccifer* data on the server in Romania, to obtain all data that came from Mrs. Clinton's server as well as Mr. Blumenthal's server.
2. Analyze all of the content of the computer IP 84.232.210.154, which appears to be different from the *Guccifer* server, although both apparently are located in the Bucharest, Romania area.
3. *Guccifer* claims in recent reports that the secret server contains about 2 Terabytes of data and represents all of his hacking efforts. We opine this statement is most likely accurate. The spreadsheet that we obtained which maps the secret server substantiates this claim, assuming a portion of it originated from the *Guccifer* server.
4. The Clinton smoking gun data document needs to be mapped back to her server to make the clear connection which has not been satisfactorily established.

5. The IP address and email addresses of Mrs. Clinton and her colleagues who used this server need to be checked to determine whether any content traced back to the server or the email address can be recovered from the Deep Web and the Dark Web sources to which we have access.
6. The recovered data content needs to be date stamped and placed in a chronological arc to triangulate against the activities of Mrs. Clinton, particularly around the time when she was dealing with the Benghazi investigation.
7. Counsel needs to determine from quality counsel with National Security experience and intelligence experts, the legal obligations by cleared persons to report and surrender data that may have overtly labeled classified data; or data that would objectively be considered classified had it been hypothetically subjected to a person possessing original classification authority.

## PHASE I SEARCH RESULTS

### Introduction and Overview

In an effort to determine whether there was evidence to indicate if a search of the open source spheres using mid-level recovery tools was fruitful, the customer requested that we begin our research on a limited basis, and provide results for Phase I only. The critical search terms are the email server MX codes, the headers or footers of the email server, or at a minimum, the domain server name which is fairly unique.

The study, a worldwide search, was done in less than 30 days and the cost was approximately \$33,000. The objective was to determine whether the server of Hillary R. Clinton was directly or indirectly entered by outside sources, and the content found within the Deep Web or the Dark Web. The client has not funded, nor authorized Phase II and Phase III, a much deeper probe that is dependent upon the results of Phase I.

The client was advised that this research was pursuant to the attorney-client privileged communications privilege and was intended for use in the pending federal litigation involving the Hillary Clinton's private email server.

The customer has agreed that the only exception to this privilege (which would otherwise be reserved only to the client and its law firm) is the discovery of any evidence whatsoever suggesting (directly, indirectly, overtly or otherwise) classified data (without regard to whether we do not possess original classification authority) had been absconded from the United States (wherever situated) and placed on an outside server or device and discovered by us.

Should this have occurred, or is suspected to have occurred, we advised the client that we have legal obligations to turn over that information as well as the context of that information to the appropriate authorities, inside or out of the Intelligence Community. (e.g., Federal Law Enforcement within the Criminal Division, as opposed to the National Security Division) of the FBI. The client has specifically agreed to this single condition or exception to the privilege.

### Specific Findings

During this phase, we were not engaged to determine who accessed the server or where its contents ultimately landed or came to final rest. However, we were able to determine that:

- (a) Sidney Blumenthal's server was directly hacked by *Guccifer* and Hillary Clinton's server was indirectly attacked by *Guccifer*, probably as a result of first hitting Mr. Blumenthal's server.
- (b) The Blumenthal content was transferred to a computer or server located south of Bucharest, Romania by *Guccifer*; but we also found this content outside of his server or computer where it still remains to this day and is under another IP address.
- (c) We confirmed that it was possible the same person or persons acting on *Guccifer*'s behalf or persons impersonating *Guccifer* did a secondary penetration of Mrs. Clinton's server on May 22, 2009.
- (d) While the first "pop" where the Clinton/Blumenthal content landed could have been at the *Guccifer* server, the place where we recovered the files containing this content was not the same server as where *Guccifer* hid the files, based upon our limited scans to date. The

reason is that this server IP address is continuing to collect to this day, and moreover, the date when the content was first seen after when *Guccifer* was apprehended and jailed in Romania. More clarification of this point is needed at Phase II as to who truly are the creator and owner of the server where we found this content and report it here.

(c) We believe that the IP address where we found the files is 84.232.210.154, which is not a server, but is actually a computer using an application that accesses files on Peer-to-Peer localities. In essence, the computer is utilizing the Direct Connect P2P application which disclosed the content of the computer to others on an open network known as the Deep Web or Dark Web. Upon checking IP address 84.232.210.154, we recovered in excess of 37,000 files, of which at least 200 appear to have come from Mr. Blumenthal's computer. Of the 200+, we verified the authenticity of a representative sample of over 20 having been documents authored by Mr. Blumenthal, and sent to Mrs. Clinton, according to the headers.

(f) From a counter-intelligence perspective, if classified data is located on the above IP address, it represents a major problem for the National Security interests of the United States because by its very nature, data falling into the Dark Web from a computer means it is "open source" and therefore publicly available. In essence, if we found it, others have found it – nothing that we are doing in our trawling represents a "secret sauce" or source. Our tools used may be different or better from a forensic trawling perspective, but these resources are generally available.

(g) There is subjective evidence suggesting that Mr. Blumenthal and two others may have had a motive to present to Mrs. Clinton "tree-shaking" Intelligence SITREPs, hoping for a possible quid-pro-quo of sorts, but this is our unconfirmed, raw assessment. The possible deal may have included participation in the rogue national judgment recovery program for the Libyan Opposition Government, in exchange for the State Department Intelligence File that existed on the Qaddafi family asset seizure.

(h) There is objective evidence to indicate that a person identified as [redacted] telephone [redacted] (circa 10 January 2012) began to solicit Senior Intelligence Analysts with experience in repatriation of assets plundered by the Qaddafi family. This person began the solicitation process on approximately January 25<sup>th</sup> 2012, claiming that he led was dealing with representatives of a "high level political types in the US within the State Department" and that he personally had high level contacts within the new Libyan Opposition Government that he would have a contract with to begin the repatriation process. [redacted] has a rather controversial history within the US Intelligence Community, particularly at [redacted]. His links to [redacted] was one of the prime operatives in Libya. Notwithstanding his reputation in the US Intelligence Community, he was believed to have highly placed contacts within Libya which could have been mined for creation of a Rogue Nation Asset Recovery program, but for his limited technical and intelligence analyst resources.

(i) After the above scheme floundered, others representing the Libyan Opposition Coalition Government sought to re-start the contract that we believe Mr. Blumenthal and his colleagues had. This re-ignited effort occurred as recently as December 2015.

#### *Deep Web Search Methodology*

Searching the Deep Web and the Dark Web is not the same as conventional searching using a normal web browser. One not only must have a different tool, but also have the tool with the correct protocol to access a specific site. Often, to gain access to an IP address containing hidden files, such as what we see here, the protocol tool is uniquely different and it often takes considerable effort to find the correct, corresponding protocol tool so that one has complete and unfettered access.

b6  
b7C

Employment of these protocols is done by the owner of the site where the files are located in order to maintain the integrity and security of the site where the hidden files are located and to keep "prying eyes" out.

Once the location of the files is identified, the next step in the process is gaining access to the site, obtaining, collecting and acquiring all of the files, and downloading them to a safe and secure environment.

In this case, the computer of Sidney Blumenthal was positively identified as the host of many documents sent to the server of Hillary Clinton and others from the Clinton Foundation. Mr. Blumenthal's server was successfully attacked by Marcel Lazar Lehel, also known as *Guccifer* or "Small Fume," originally from Bucharest. While one spreadsheet shows that over 37,000 files were found, only a full analysis of the spreadsheet will reveal all of the files traced back to Mrs. Clinton's server directly, or to that of Mr. Blumenthal.<sup>†</sup>

It was believed initially, that the content was the hidden *Guccifer* server that he kept and maintained in secret, or allowed to continue to run and collect data from various sources whilst he was incarcerated. However, this assessment seems both farfetched and not particularly logical. More likely, the content we discovered at the IP address cited above is an unknown person that originally collected some of the Blumenthal/Clinton content from the *Guccifer* server, and then moved it to where we located it. If this assessment is correct, it is particularly damning, because it means that if the content contains national security information, it has escaped the first landing spot, and has migrated to an unknown destination.

We assess that it is possible *Guccifer* entered the Blumenthal computer several times, first through Blumenthal's AOL account. It is not clear whether *Guccifer* targeted Blumenthal because he represented an opportunity of interest, or because a foreign service directed him to the account. Also, it is not clear whether the account was entered after he first entered the Clinton server or that of someone else on the Clinton domain server. During Phase II, much additional information can be obtained on the sequence, timing and chronology of when the two servers in question were accessed and in what order and how many times.

What is known is that *Guccifer* is a wholesale, sociopathic hacker who conducts pernicious attacks, not for reasons of ideology or retaliation – rather he does it for money and to sell data to the highest bidder. As a result, he was indicted and jailed in Romania and at the behest of the US Justice Department and the FBI, extradited to the United States where he was also charged and where he recently pled guilty. While *Guccifer* was tagged for extradition by the FBI before the Clinton email scandal erupted into the public domain, it is curious that his transfer comes exactly at the time when the FBI most needs him, when they are finalizing their prosecutive memo to the Justice Department.

*Guccifer* hopscotched among the accounts of victims such as [REDACTED]

[REDACTED]

b6  
b7c

<sup>†</sup> For additional information on files extracted from the server of Sidney Blumenthal by "Guccifer only", and found on a Password Protected, encrypted server of "Guccifer" in Bucharest, Romania, please see Attachment #3 Blumenthal Server Traced to Bucharest First Attack

b6  
b7C

Additionally, *Guccifer* further sorted the mail so that he could download all Word files attached to e-mails sent to Clinton, as well as the emails, .pdf documents as well as .rar and .zip files. We created a spreadsheet of the entire drive of where the Blumenthal as well as the Clinton files landed, a private server in Bucharest, and identified nearly 37,000 records, not all of which came from the Blumenthal/Clinton Server, but represent the fruits of the *Guccifer*'s labors over time.

Moreover, the content is so massive that it would take a high quality Senior Intelligence Analyst to do all of the post-processing analysis upon such a large bulk of data. One search revealed that an attack was done upon Mr. Blumenthal's server on July 5<sup>th</sup> 2014 at 07:12 (Bucharest Time), and yielded many references to "HRC" within the spreadsheet.

[illegible]



## List of Files Recovered from Sidney Blumenthal's File Came From Hill's Clinton Server

Examples of just a few of the indexed entries from the spreadsheet that represent e-mails that were the consequence of a "direct attack" upon Mrs. Clinton and were sent to Mr. Blumenthal are found below:

file memo_algeria_081713.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	3b1939466080234e2ac38933e53134064	7/5/2014 7:12
file memo_alexandria_081813.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	8d1a4c951700b826c4d902526125a69782	7/5/2014 7:12
file memo_Comprehensive_Report_on_Sidney_081913.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	2e1c6466b6e737a3b700690300b763137504	7/5/2014 7:12
file memo_egypt_082013.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	00282b182e616b8ac0a0f50089a4f6dc176	7/5/2014 7:12
file memo_Euro_Fin_082113.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	3ae16a6c064184226789aacc166778053a4	7/5/2014 7:12
file memo_Georgia_082213.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	4c4015751050e4e578038a18018837d2d964	7/5/2014 7:12
file memo_Iraq_082313.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	012406a87d3661a7a28b27786c2d583a0	7/5/2014 7:12
file memo_Libya_082413.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	94415d1d7b9180b0e077e8d2e642e4389	7/5/2014 7:12
file memo_Libya_082513.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	c0d47e0d1b0785d1d6e0e0e255a0c0b	7/5/2014 7:12
file memo_Libya_082613.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	505301578b1a1d5d817d488f1c079e47	7/5/2014 7:12
file memo_Libya_082713.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	80f4209578c18074e35d524e17e38402	7/5/2014 7:12
file memo_Libya_082813.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	d37e70e3a243087602381730215817	7/5/2014 7:12
file memo_Libya_082913.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	6e6f0c011b12e7a66b411e1b0a0397a887	7/5/2014 7:12
file memo_Libya_083013.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	8ae302e6110b0f6d1d80d06121b81447	7/5/2014 7:12
file memo_Libya_083113.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	042ca0b0e5785d1a77279491504a12	7/5/2014 7:12
file memo_Libya_083213.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	085d1a7546e4e7d1d3d3d8b7760c3881	7/5/2014 7:12
file memo_Libya_083313.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	0b27c7c8441b1a1a0a991a0c0d1a1a0a	7/5/2014 7:12
file memo_Libya_083413.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	946e3f530e0b176d1a1730c1b372880d	7/5/2014 7:12
file memo_Libya_083513.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	19b881d4e46745ac78113d8d196581	7/5/2014 7:12
file memo_Libya_083613.docx	Sidney Blumenthal	application/vnd.openxmlformats-officedocument.wordprocessingml.document	ez4d743447407e0d81114610486e09b	7/5/2014 7:12

It is not clear whether the cited memos were created by Mr. Blumenthal and sent to Mrs. Clinton or whether she was the original creator of the memos and sent them to Mr. Blumenthal. What is abundantly clear is that sensitive memos between the two were found on the Dark Web and in a foreign country.

Thus, the above chart meets or exceeds the objective and mission of the Phase I inquiry. Each of the items cited in the sample above could be recovered with additional research and work, and then traced back to the creator. The moment that this type of data, using these kinds of key words, phrases, hashtags, and addresses appear in the Dark Web, foreign intelligence services would become aware, and then mine and exploit them.

### Suspected Location of IP Address 84.232.210.154

While we cannot determine the exact location where the computer is that links to IP address 84.232.210.154, the Internet Service Provider for the box is located at 71-75 Dr. Staicovici, Bucharest, Romania, telephone +40 21 30 10 888, telefax number +40 21 30 10 892.

This company is known as Romania Data Systems NOC, and its contact email address appears to be [dan.epure@rcs-rds.ro](mailto:dan.epure@rcs-rds.ro). The IP location, according to one report source is listed as Chiajna Rcs and Rds Residential, but this has not been checked through ground sources.

IP Location	Romania Chiajna Rcs & Rds Residential
ASN	AS8708 RCS-RDS RCS & RDS SA, RO (registered Mar 11, 1998)
Resolve Host	84-232-210-154.rdsnet.ro
Whois Server	whois.ripe.net
IP Address	84.232.210.154

0554-2600

85,232,210,154 Tracemate		
Min	T1	TRM1
1	6,255	Commodity 3 (material in box)
2	6,256	Commodity 3 (material in box)
3	6,257	Commodity 3 (material in box)
4	6,258	Commodity 3 (material in box)
5	6,259	Commodity 3 (material in box)
6	6,260	Commodity 3 (material in box)
7	6,261	Commodity 3 (material in box)
8	6,262	Commodity 3 (material in box)
9	6,263	Commodity 3 (material in box)
10	6,264	Commodity 3 (material in box)
11	6,265	Commodity 3 (material in box)
12	6,266	Commodity 3 (material in box)
13	6,267	Commodity 3 (material in box)
14	6,268	Commodity 3 (material in box)
15	6,269	Commodity 3 (material in box)
16	6,270	Commodity 3 (material in box)
17	6,271	Commodity 3 (material in box)
18	6,272	Commodity 3 (material in box)
19	6,273	Commodity 3 (material in box)
20	6,274	Commodity 3 (material in box)
21	6,275	Commodity 3 (material in box)
22	6,276	Commodity 3 (material in box)
23	6,277	Commodity 3 (material in box)
24	6,278	Commodity 3 (material in box)
25	6,279	Commodity 3 (material in box)
26	6,280	Commodity 3 (material in box)
27	6,281	Commodity 3 (material in box)
28	6,282	Commodity 3 (material in box)
29	6,283	Commodity 3 (material in box)
30	6,284	Commodity 3 (material in box)
31	6,285	Commodity 3 (material in box)
32	6,286	Commodity 3 (material in box)
33	6,287	Commodity 3 (material in box)
34	6,288	Commodity 3 (material in box)
35	6,289	Commodity 3 (material in box)
36	6,290	Commodity 3 (material in box)
37	6,291	Commodity 3 (material in box)
38	6,292	Commodity 3 (material in box)
39	6,293	Commodity 3 (material in box)
40	6,294	Commodity 3 (material in box)
41	6,295	Commodity 3 (material in box)
42	6,296	Commodity 3 (material in box)
43	6,297	Commodity 3 (material in box)
44	6,298	Commodity 3 (material in box)
45	6,299	Commodity 3 (material in box)
46	6,300	Commodity 3 (material in box)
47	6,301	Commodity 3 (material in box)
48	6,302	Commodity 3 (material in box)
49	6,303	Commodity 3 (material in box)
50	6,304	Commodity 3 (material in box)
51	6,305	Commodity 3 (material in box)
52	6,306	Commodity 3 (material in box)
53	6,307	Commodity 3 (material in box)
54	6,308	Commodity 3 (material in box)
55	6,309	Commodity 3 (material in box)
56	6,310	Commodity 3 (material in box)
57	6,311	Commodity 3 (material in box)
58	6,312	Commodity 3 (material in box)
59	6,313	Commodity 3 (material in box)
60	6,314	Commodity 3 (material in box)
61	6,315	Commodity 3 (material in box)
62	6,316	Commodity 3 (material in box)
63	6,317	Commodity 3 (material in box)
64	6,318	Commodity 3 (material in box)
65	6,319	Commodity 3 (material in box)
66	6,320	Commodity 3 (material in box)
67	6,321	Commodity 3 (material in box)
68	6,322	Commodity 3 (material in box)
69	6,323	Commodity 3 (material in box)
70	6,324	Commodity 3 (material in box)
71	6,325	Commodity 3 (material in box)
72	6,326	Commodity 3 (material in box)
73	6,327	Commodity 3 (material in box)
74	6,328	Commodity 3 (material in box)
75	6,329	Commodity 3 (material in box)
76	6,330	Commodity 3 (material in box)
77	6,331	Commodity 3 (material in box)
78	6,332	Commodity 3 (material in box)
79	6,333	Commodity 3 (material in box)
80	6,334	Commodity 3 (material in box)
81	6,335	Commodity 3 (material in box)
82	6,336	Commodity 3 (material in box)
83	6,337	Commodity 3 (material in box)
84	6,338	Commodity 3 (material in box)
85	6,339	Commodity 3 (material in box)
86	6,340	Commodity 3 (material in box)
87	6,341	Commodity 3 (material in box)
88	6,342	Commodity 3 (material in box)
89	6,343	Commodity 3 (material in box)
90	6,344	Commodity 3 (material in box)
91	6,345	Commodity 3 (material in box)
92	6,346	Commodity 3 (material in box)
93	6,347	Commodity 3 (material in box)
94	6,348	Commodity 3 (material in box)
95	6,349	Commodity 3 (material in box)
96	6,350	Commodity 3 (material in box)
97	6,351	Commodity 3 (material in box)
98	6,352	Commodity 3 (material in box)
99	6,353	Commodity 3 (material in box)
100	6,354	Commodity 3 (material in box)

[illegible][illegible]



# Quick Stats

IP Location: Romania Chiajna Rcs & Rds Residential

ASN: AS8708 RCS-RDS RCS & RDS SA, RO (registered Mar 11, 1998)

Resolve Host: 84.232.210.154.rdsnet.ro

Whois Server: whois.ripe.net

IP Address: 84.232.210.154

Abuse contact for 84.232.192.0 - 84.232.213.255  
to: abuse@rds.ro

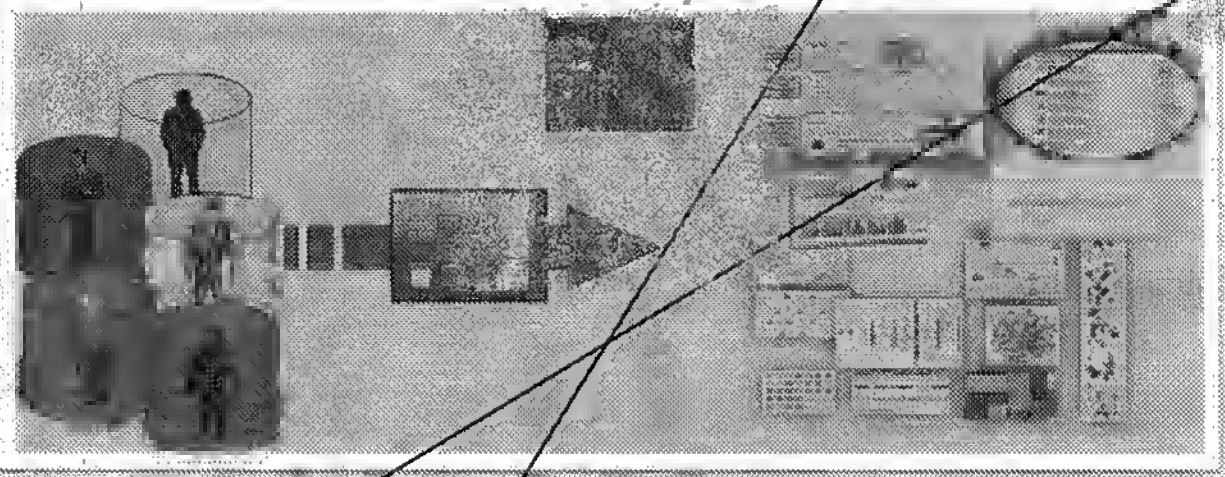
inetnum: 84.232.192.0 - 84.232.213.255  
netname: RO-RESIDENTIAL  
descr: RCS & RDS Residential  
city: Bucuresti  
country: RO  
admin-c: RDS-RIPE  
tech-c: RDS-RIPE  
tech-n: RDS2013-RIPE  
status: ASSIGNED PA  
notify: notify-ripe@rdsnet.ro  
mnt-by: AS8708-MNT  
mnt-lower: AS8708-MNT  
created: 2013-08-12T00:00:00Z  
last-modified: 2013-08-12T00:00:00Z  
source: RIPE

role: Romania Data Systems NOC  
address: 21-15 DE STELCOVICI  
address: BUCHAREST, ROMANIA  
phone: +40 21 30 10 680  
fax-no: +40 21 30 10 682  
e-mail: nps@rds.ro  
abuse-mailbox: abuse@rds.ro  
admin-c: REPUI-RIPE  
admin-c: VIGIO-RIPE  
tech-c: REPUI-RIPE  
tech-c: VIGIO-RIPE  
nir-hdl: RDS-RIPE  
mnt-by: AS8708-MNT

remarks: | ABUSE CONTACT: [abuse@rds-rds.ro](mailto:abuse@rds-rds.ro)  
 IN CASE OF HAAR ATTACKS,  
 remarks: | ILLEGAL ACTIVITY, VIOLATION, SC  
 AMS, PROBES, SPAM, ETC.  
 remarks: | !! PLEASE DO NOT CONTACT OTHER PER  
 SONS FOR THESE PROBLEMS !!  
 remarks: | -----  
 created: 2010-01-01T00:00:00Z  
 last-modified: 2015-10-07T05:29:53Z  
 source: RIPE  
 type: RDS-RDS  
 address: 71-75 Dr. Stăncovici  
 address: Bucharest / ROMANIA  
 phone: +40 21 30 10 888  
 fax-no: +40 21 30 10 898  
 e-mail: [dan.epure@rds-rds.ro](mailto:dan.epure@rds-rds.ro)  
 abuse-mailbox: [abuse@rds-rds.ro](mailto:abuse@rds-rds.ro)  
 admin-c: GEPUL-RIPE  
 tech-c: GEPUL-RIPE  
 nic-hdl: RDS2012-RIPE  
 mnt-by: RDS-MNT  
 remarks: | -----  
 remarks: | Please use [abuse@rds-rds.ro](mailto:abuse@rds-rds.ro)  
 for complaints and only after  
 remarks: | you have tried contacting directly  
 our customers according  
 remarks: | to the details registered in RIPE  
 Database.  
 remarks: | -----  
 remarks: | DO NOT CALL, FAX, OR CONTACT US BY  
 ANY OTHER MEANS EXCEPT  
 remarks: | [abuse@rds-rds.ro](mailto:abuse@rds-rds.ro)  
 remarks: | -----  
 created: 2012-01-24T08:33:39Z  
 last-modified: 2013-05-11T03:16:10Z  
 source: RIPE  
 date: 2012-12-07/17  
 descr: RDS & RDS S.A.  
 origin: AS2796  
 notify: [npe@namacit.com](mailto:npe@namacit.com)  
 mnt-by: AS2796-MNT  
 created: 2006-06-09T13:04:06Z  
 last-modified: 2006-06-09T13:04:06Z  
 source: RIPE

In real terms, every person today has a data fingerprint, much like a skin fingerprint. As people operate in the e-commerce world, the "Data DNA" of their digital fingerprint leaves an indelible mark that is rarely deletable. Spending patterns, financial transactions, telephone call pattern analysis, credit card transactions, travel habits, subscriptions to magazines and online computer behavior cannot be altered. While people often try to conceal or obfuscate their tracks, computer forensics can be employed to detect their connection.

Humans today translate into digital images, both structured and unstructured. Data, pictures, sounds, cyber visits – all of it compose a person's data DNA that is unique to that person. It looks something like the illustration below:



Advanced analytics are used to do data extraction, recognizing that:

- ◆ **88% of the world's digital content is unstructured or semi-structured, to include:**
  - ◆ Newspapers data sources
  - ◆ Financial statements contained deep within web sites
  - ◆ Government reports that are both open and closed
  - ◆ Press releases on the surface Web
  - ◆ Websites, both open and closed
  - ◆ Emails that are dumped into the public domain
- ◆ **Semantic extraction is typically used to**
  - ◆ Discover entities and identify their structural ownership and links
  - ◆ Discover relationships between entities
  - ◆ Discover events
  - ◆ Taxonomy generation
  - ◆ Categorize documents



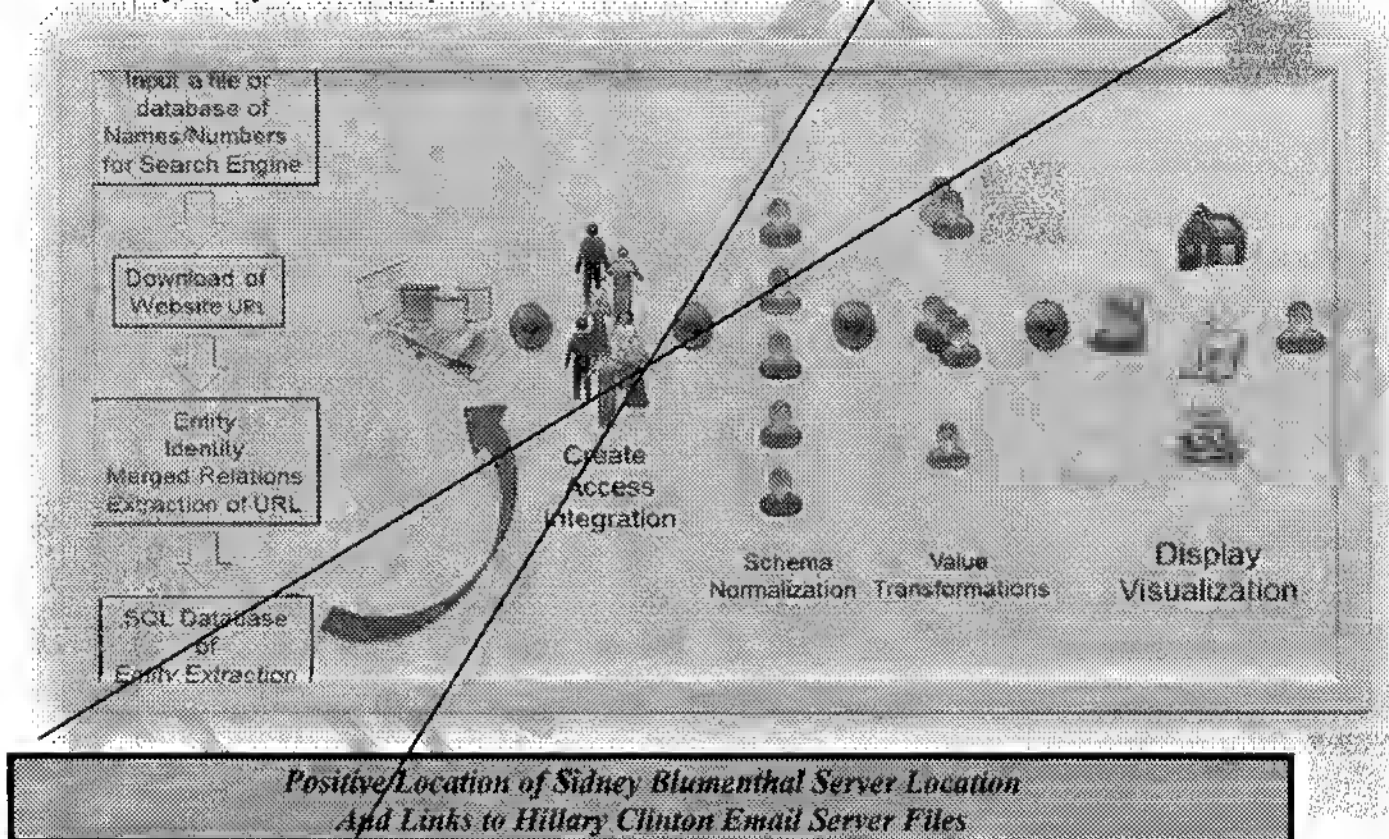
◆ A high-performance data-extraction system that consists of

- ◆ A design-time *compiler*
- ◆ A run-time *engine*
- ◆ A powerful *Integrated Development Environment (IDE)*
- ◆ Several utility programs

◆ Semantic extraction is typically used to

- ◆ Discover entities
- ◆ Discover relationships between entities
- ◆ Discover events
- ◆ Categorize documents

Technically, entity extraction operates somewhat in this manner:



***Positive Location of Sidney Blumenthal Server Location  
And Links to Hillary Clinton Email Server Files***

As stated at the outset, this investigation is a multi-phase project starting with the Phase I inquiry, and once the results are obtained, we can probe the leads deeper and trace back related information, if any, to the original source. Based upon the spreadsheets showing that several direct and indirect attacks were executed upon Mr. Blumenthal and Mrs. Clinton jointly, we focused first on Mr. Blumenthal's background in an effort to identify the server location.

**Sidney Stone Blumenthal** born [redacted] and currently resides at [redacted] telephone [redacted] as well as [redacted] [redacted] Mr. Blumenthal's Social Security account number is listed as [redacted] originally issued from [redacted] We note that he traces to numerous iterations of his given date of birth, to include [redacted] as well as [redacted]

b6  
b7C

Aside from his known AOL email address, Mr. Blumenthal also traces to [redacted] which was also hacked around July 2015.

b6  
b7C

We checked another database<sup>2</sup> and found some of the reported IP addresses that were linked to Mr. Blumenthal's email addresses, as well as his home address, based upon a search of his Social Security account number. The registry is abstracted below:

Name	Address	SSN / DOB	Phone	Flags									
				AR	BK	CR	EV	JG	PL	SO	TL	WW	
BLUMENTHAL SIDNEY S	[redacted] 3x Reported: 07/11/2015 - 05/29/2016 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]	Landline: [redacted]	N	N	N	N	N	N	N	N	N	N
BLUMENTHAL SIDNEY S AKA: SIDNEY BLUMENTHAL AKA: SIDNEY BLUMENTHAL	[redacted] 1x (POSSIBLE HIGH RISK) Reported: 05/09/2000 - 01/30/2014 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]		N	N	N	N	N	N	N	N	N	N
E-mail: [redacted] E-mail: [redacted] E-mail: [redacted]	IP address: [redacted] IP address: [redacted] IP address: [redacted]		Phone: [redacted] Phone: [redacted] Phone: [redacted]	Reported: 10/18/2011 Reported: 10/06/2011 Reported: 04/25/2009									

b6  
b7C

We also expanded the search to a scan of the address itself [redacted]  
[redacted] We obtained the following results:

b6  
b7C

Search Criteria

Address: [redacted]  
City: [redacted]  
State: [redacted]  
Zip: [redacted]

Flags: Arrests, Bankruptcies, Criminal Records, Evictions, Civil Judgments, Professional Licenses, Sex Offender Records, Tax Liens, Warrants  
Options: E-mail Records, High Risk Addresses

b6  
b7C

Name	Address	SSN / DOB	Phone	Flags									
				AR	BK	CR	EV	JG	PL	SO	TL	WW	
BLUMENTHAL SIDNEY S	[redacted] 3x Reported: 07/11/2015 - 05/29/2016 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]	Landline: [redacted]	N	N	N	N	N	N	N	N	N	N
AKA: [redacted] AKA: [redacted] AKA: [redacted] AKA: [redacted]	[redacted] 1x Reported: 03/14/2014 - 03/14/2014 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]		N	N	N	N	N	N	N	N	N	N
AKA: [redacted] AKA: [redacted] AKA: [redacted]	[redacted] 1x Reported: 01/08/2006 - 01/08/2006 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]		N	N	N	N	N	N	N	N	N	N
[redacted] [redacted] [redacted]	[redacted] 1x Reported: 02/28/1993 - 02/28/1993 County: [redacted]	Issued: [redacted] DOB: [redacted] Age: [redacted]		N	N	N	N	N	N	N	N	N	N

b6  
b7C

For more information, please see Attachment #6 [redacted] Syd Blumenthal IP and SSN Scan

b6  
b7C

We created a chart of known or suspected relatives, friends, associates and acquaintances, based upon his digital profile, which is summarized at page 310-312 of the basic [redacted] report attached.<sup>3</sup>

b6  
b7C

Mr. Blumenthal is an American journalist, activist, writer and former political aide of President Bill Clinton as well as a long-time confidant to Hillary Clinton; and a journalist, especially on American politics and foreign policy. He was editor of several departments and wrote for a number of publications including *The Washington Post*, *Vanity Fair*, and *The New Yorker*. He is the father of Max Blumenthal who is also a journalist and political activist.

Mr. Blumenthal was born in Chicago, to Claire (née Stone) and Hyman V. Blumenthal. He earned a BA in sociology from Brandeis University in 1969, and started his career in Boston as a journalist who wrote for *The Boston Phoenix* and *The Real Paper*, two alternative weeklies of the day. Mr. Blumenthal resides in Washington DC but also has offices and connections to California and Chicago.

Mr. Blumenthal has also used numerous iterations of his name, to include:

SSN:

[redacted]

issued in

[redacted]

AKAs:

1) BLUMENTHAL, SIDN

SSN: [redacted]

DOB: [redacted]

2) BLUMENTHAL, SIDNEY S

3) BLUMENTHAL, SIDN

4) BLUMENTHAL, SIDNEY S

SSN: [redacted]

DOB: [redacted]

5) BLUMENTAL, SIDNEY

SSN: [redacted]

DOB: [redacted]

6) BLUMENTAL, SIDNEY

7) BLUMENTHAL, SIDNEY S

DOB: [redacted]

8) BLUMENTHAL, SIDNEY

SSN: [redacted]

9) BLUMENTHAL, SIDNEY S

SSN: [redacted]

10) BLUMENTAL, SIDNEY

SSN: [redacted]

11) SIDNEY, BLUMENTHAL

b6  
b7C

Based upon our initial research, it appears that Mr. Blumenthal's computer or server had been connected at [redacted]. However, we do not know at this juncture whether he used a lap top, desk top, or if the computer was portable (such as a device) at the time of the attack.

b6  
b7C

We note that Mr. Blumenthal has a number of devices that he uses, to include phones, but this attack was not done upon a mobile device. Every indication is that it was a static and stationary server, such as a laptop or desk top. We checked a number of databases and found that Mr. Blumenthal traces to a number of other addresses in the Washington DC area, to include:

<sup>3</sup> For additional information regarding locations of Sidney Blumenthal, and his servers and email addresses, please see Attachment #1 SYD BLUMENTHAL Basic [redacted] Report

TransUnion	Not Available
Experian	
Experian Gateway	
Historic Credit Bureau	
Deed	
TransUnion	
Historic Credit Bureau	
Experian	
Experian Gateway	
Phone Record	Not Available
Phone Record	Not Available
Historic Credit Bureau	Not Available

### *Historical Background of Sidney Blumenthal and Connections to Hillary Clinton*

Mr. Blumenthal has long time connections to both President as well as Mrs. Clinton. As stated, he served as assistant and senior adviser to Bill Clinton from August 1997 until January 2001. His responsibilities included advising the President on communications and public policy as well as researching information in the general media about the White House. He became a major figure in the grand jury investigation that ended in the impeachment of President Clinton.

While working on the White House Staff, Mr. Blumenthal was known for his loyalty to the Clintons, and for attacks on their adversaries, which is one reason Rahm Emanuel, original chief of staff for President Obama, barred Blumenthal from holding a position in Hillary Clinton's State Department.

After the House Judiciary Committee and the United States House of Representatives impeached Clinton, the matter then passed to the United States Senate. Mr. Blumenthal was one of four witnesses called to testify before the Senate. No live witnesses were called; the four were interviewed on videotape.

His testimony addressed the key "lie": that President Clinton was allegedly pressuring Betty Currie and Mr. Blumenthal to attest that it was Ms. Lewinsky who initially pursued the President, not vice versa. Ms. Lewinsky stated she was the one who instigated the relationship. With the assistance of other evidence and arguments, the Senate acquitted President Clinton of perjury and impeachment proceedings ended.

In 2008 Mr. Blumenthal joined the Hillary Clinton presidential campaign as a "Senior Advisor" in November 2007. While on a trip to advise Clinton on her presidential campaign,

We find it curious that at Attachment #2, there is no mention of [redacted] which normally would be reported. It is possible that he was able to [redacted] not an easy effort.

According to a report in the New York Times, "Emanuel talked with Mrs. Clinton ... and explained that bringing Mr. Blumenthal on board was a no-go. The bad blood among his colleagues was too deep, and the last thing the administration needed, he concluded, was dissension and drama in the ranks. In short, Mr. Blumenthal was out...."

# THE NEW YORK PUBLIC LIBRARY

The client should note that separately, there is evidence that tends to suggest that the entire Benghazi aspect of the Clinton probe maybe somewhat "objectively misplaced" in that our evidence shows that Mr. Blumenthal was involved with a group of intelligence professionals seeking to repatriate asset which were plundered and then exfiltrated by the Gaddafi family and hidden in various offshore localities. One of the devices used by his lawyers and advisors was the infamous Panama Papers law firm that has recently been referenced in the news. This program is better known as *Rogue National Judgment Recovery Litigation*, for which we have much experience, sources, and knowledge generally.

During the last several years, the new Libyan coalition government had a strong desire to hire a group of professionals that could identify other Gaddafi family assets plundered from the country which is suspected of being about \$66 billion. Mr. Blumenthal touted his and his associate's ability to find the money and thus become the preferred contractor for the coalition government.

4 For additional information, please see a small sample of memos sent from Sidney Blumenthal to Hillary Clinton that represent "bait" to entice State Department to release intelligence file on assets recovered, Attachment #5 Sidney Blumenthal Sample Memos to HRC Regarding Libya



classified intelligence; combined with the Libyan Central Bank intelligence use the combined files and data silos to track down the missing money for the coalition government.

As an illustration of how profitable this Program can be, since the Blumenthal group had a contingency contract with the coalition government, if they found just \$1 billion in assets<sup>3</sup> and the contingency agreement was just 10% of the funds recovered (which is extremely conservative and considerably below industry standards), it would mean the group would earn a windfall of \$100 million gross.

Assuming expenses of 10% of the gross, which would be extremely generous, the net to the group would be nearly \$90 million. The only obstacle separating Mr. Blumenthal and the money was the State Department intelligence; and the key to getting it was Mrs. Clinton, his long-time patron.

For these reasons, we assess that the true motivation behind Mr. Blumenthal's willingness to move mountains of data about Libya to Mrs. Clinton was all about the money and to get access to or actually obtain the State Department intelligence file, notwithstanding the fact that it would be highly illegal for the file to be released to a private citizen.

Part of the reason that we make this assessment is that we know a number of the members of the proposed Blumenthal team who reached out to intelligence professionals familiar with rogue nation judgment recovery work and particularly those that are experts in tracing missing money. We also are aware that this team created a corporate vehicle offshore; and we know that a draft agreement was crafted between the team and the coalition government to work on the project. What we do not know is whether the team was actually operationalized or if the attendant publicity surrounding the email server effectively shut down the Blumenthal team's efforts.

Above we opined the Blumenthal memos had dubious sourcing. The *New York Post* asserted that Blumenthal's "intel was shoddy, with basic errors like mixing up Libyan politicians with similar names. In one instance, Blumenthal asserted that a businessman named [REDACTED] was among 'the most influential' of the Libyan prime minister's new economic advisers—without mentioning that Blumenthal was advising a group of contractors courting [REDACTED] as a potential business partner."

b6  
b7c

The House Select Committee on Benghazi, headed by Representative Trey Gowdy (R-SC) served a subpoena on Blumenthal on May 19, 2015 for a deposition to be held on June 3, according to Reuters. Blumenthal's name came up during the October 22, 2015 full committee public questioning of Hillary Clinton regarding the Benghazi incident, as one of the alleged sources of Hillary Clinton's intelligence. During this hearing Democratic members asked that Blumenthal's deposition transcript be made public so that comments regarding his involvement could be placed in context. The motion was defeated by a voice vote, followed by a roll call vote along party lines.

Mr. Blumenthal has a dubious litigation history: In 1997, Blumenthal instigated a \$30 million libel lawsuit against Internet blogger Matt Drudge (and AOL, who had hired Drudge) stemming from a false claim Drudge had made of spousal abuse attributed to "top GOP sources". Drudge retracted the story later, saying he had been given bad information. In *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998), the court refused to dismiss Blumenthal's case for lack of personal

<sup>3</sup> Published reports suggest that the Coalition Government believes that between \$60 billion and \$100 billion in assets was absconded by the Ghaddafi family and exfiltrated from the country and laundered.

jurisdiction. Drudge later publicly apologized to the Blumenthals. Mr. Blumenthal dropped his lawsuit and eventually reached a settlement involving a payment to Drudge over having missed a deposition. In his book, *The Clinton Wars*, Blumenthal claimed he was forced to settle because he could no longer financially afford the suit.

#### *Global Scan Search*

We did a very basic scan on Mr. Blumenthal,<sup>6</sup> mostly in an effort to isolate the email addresses, IP addresses, and identity of devices that he was using to communicate with Mrs. Clinton.

A Global Scan could not be done on Mrs. Clinton because of a number of technical, legal and practical reasons, but every indication is that her server was located at her home, but copies were maintained in later years at various hosting companies.

For purposes of this study, the issue is whether Mrs. Clinton's server was impermissibly entered by unauthorized persons either before or after the entry of Mr. Blumenthal's server.

It is our opinion, based upon experience in cyber defensive and offensive operations, that once Mr. Blumenthal's server was compromised and data was found that included many emails, attachments, and other data which originated from Mrs. Clinton's such persons would immediately target Mrs. Clinton's server.

#### *Rogue National Judgment Recovery Work - Inspection Concluded*

As discussed above, we understand that Mr. Blumenthal and others were involved in the Rogue National Judgment Recovery litigation as it pertains to Libya generally and the Qaddafi family specifically. As stated above, there is evidence<sup>7</sup> to suggest that one of the possible reasons that Mr. Blumenthal was engaging with Mrs. Clinton on matters related to Libya was to involve her in a "quid-pro-quo" relationship whereby he would trade intelligence from HUMINT sources in exchange for access to the State Department Intelligence Bureau file on missing Ghaddafi money.

By way of brief background, in some quarters of the legal community today, there are law firms which participate in Rogue National Judgment Recovery litigation. This type of legal work involves filing actions against middle-level political, military and intelligence persons who, having plundered a nation's treasury for personal gain, but no longer enjoy any form of diplomatic immunity. The Libyan Opposition Government had strong evidence that the Ghaddafi regime had absconded with somewhere between \$60 billion and \$100 billion dollars using a number of devices, vehicles and straw persons.

As such, the Libyan Opposition Government was soliciting law firms and intelligence operators to assist them to recovery the missing money and repatriate it to the Government.

<sup>6</sup> For additional information on Sidney Blumenthal, including location of his email accounts and servers, please see Attachment #1 SYD BLUMENTHAL Basic   Report

<sup>7</sup> We note here that the evidence is in part subjective, but there are some objective clues that support this theory as a motive. Much of this section is based upon assessment by qualified intelligence analysts, but requires much additional research at Phase II in order to either substantiate this theory or set it aside.

There is information suggesting that Mr. Blumenthal, Mr. Tyler Drumheller, (deceased 2 August 2015) born 12 April 1952, and Mr. William D. Murphy had formed a relationship whereby they contracted with the Opposition Government to try and identify, locate, and recover the missing money, in concert with a law firm that does this type of work.<sup>8</sup>

Mr. Drumheller, formerly the Chief of the European Division of the CIA, and following his retirement created a private intelligence gathering service.

Mr. Drumheller and Mr. Blumenthal have a long-time relationship that goes back to at least 2007, when Mr. Blumenthal wrote about claims that Mr. Drumheller had information from a source identified as [REDACTED] of Iraq who claimed that Iraq did not have WMD or any components thereof. This debunked the Bush Administration's narrative for the need to invade Iraq, at least according to reporting by Blumenthal, quoting his source Mr. Drumheller, who claims the intelligence came from [REDACTED] around 2002.

b6  
b7C

Normally, the operators and the law firm work in tandem and enjoy a percentage of that which is recovered. However, someone must fund the start-up operation which can be quite expensive because it involves specialists who are experts in big data analytics, money laundering, and concealment of assets, identity resolution, and tracing of converted assets.

In this unique circumstance, Mrs. Clinton had jurisdiction over the control of the State Department Intelligence Bureau file that contained much analysis and ultimate success in freezing nearly \$30 billion in Ghaddafi money. Thus, with such a file in Mr. Blumenthal's possession, combined with what he could obtain (the Libyan Central Bank data from the Libyan Opposition) he could sling shot ahead of the opposition in finding "the missing treasure."

Assuming that another \$20 billion was identified as missing, and assuming that Mr. Blumenthal and his colleagues could use the legal writs of Moravia to freeze just \$1 billion of the \$20 billion and assuming that he was working on a 10% contingency, the net to his group would be \$100 million. But, key to such an arrangement and its success would be the State Department intelligence file; combined with the Libyan Central Bank file.

So, according to this theory, Blumenthal is sending all of these SITREPs to Mrs. Clinton in an effort to "prime the pump" and obtain the file with the argument that every dollar that his group is able to re-patriot to the Libyan government, either directly or indirectly (via the State Department) is a dollar that the US taxpayers do not have to fund.

There is also objective evidence to indicate that a person identified as [REDACTED] telephone [REDACTED] (circa 10 January 2012)<sup>9</sup> began to solicit Senior Intelligence Analysts with experience in repatriation of assets plundered by the Qaddafi family.

b6  
b7C

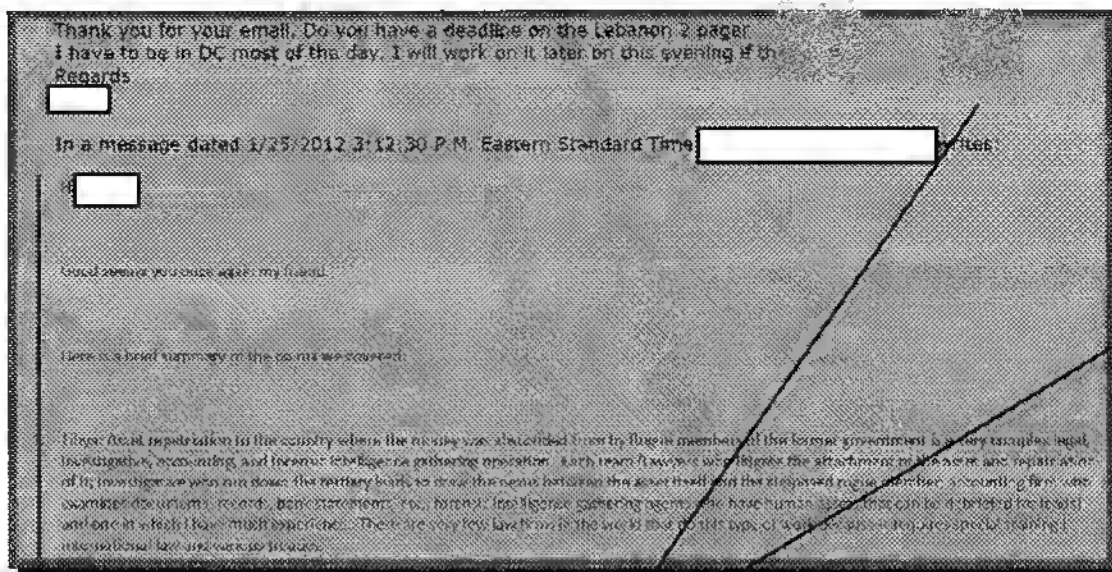
<sup>8</sup> While Mr. Murray has a long-time relationship and connection with sources in the Middle East, partly as a result of his long-time service at the CIA as a Senior Executive Officer, but also through his company Alphom Group, LLC. However, the Rogue Judgment Recovery Work assignment, it is believed (no sourcing) was not done through Alphom, but through some other offshore vehicle.

[REDACTED] has several other companies, to include [REDACTED] as well as other addresses in [REDACTED] and elsewhere. A full brief can be provided on him as necessary, but basically [REDACTED] dissent who has been a naturalized citizen in the US since around [REDACTED]. He has long-time connections to the US State Department that date to the 1990's and was actually covered as [REDACTED] where he served as [REDACTED] as he was [REDACTED]. His primary employer as [REDACTED] at the time was [REDACTED]. As such, he was also a self-styled liaison from the State Department to a number of US-based intelligence services owing to his experience in the Middle East. A full brief on him can be done, as necessary.

b6  
b7C

This person began the solicitation process on approximately January 25<sup>th</sup> 2012, claiming that he was dealing with representatives of a "high level political types in the US within the State Department" and that he personally had top-level contacts within the new Libyan Opposition Government; and that he would have a contract to assist in beginning the repatriation process.<sup>10</sup> Proof of [redacted] involvement in participating in the program, and seeking the guidance of others, is found in this post-meeting summary memo that was sent to him:

b6  
b7C



b6  
b7C

The dates when these contacts were made by [redacted] fit the time line of when Mr. Blumenthal was crafting the memos regarding Libya and other issues to Mrs. Clinton. While he never overtly states that he is need of information regarding Qaddafi plundered assets; the memos clearly contain language that is amateurish, would not inspire a lot of faith and credence by Senior Intelligence Analysts that put together all-source HUMINT and SIGINT packages for planners and policy makers.

b6  
b7C

As recently as 2014, according to published reports, [redacted] is quoted as claiming he had a direct contractual relationship with the Libyans to track down "assets that had been spirited out of the country by Gaddafi's inner circle". One of the leads that he was focusing on at the time was the Aman Bank, which allegedly was used by the family as an exfiltration vehicle.

b6  
b7C

Sourcing embellishments and characterizing the level of access, and the placement of HUMINT sources, and claiming multiple unconnected HUMINT and compartmented intelligence is a dubious practice. Reports Officers simply do not craft SITREPs or presentations using these kinds of characterizations.

Rather, the ring to these memos is that it is being done to "shake and bake" and provide Mrs. Clinton fodder for arguing that an exchange of data might inure to the benefit of the US (looking at it in the light most favorable to the parties implicated) Community and the American people, as well as the Libyan Transitional Government who were totally reliant upon US funding and strength.

<sup>10</sup> Indeed, unbeknownst to this author at the time (January 2012) [redacted] was – it is now suspected – trying to assemble a team of former high level CIA operatives with Middle East experience to help him round out the "technical team". In January 2012 [redacted] did not state to this author that he was working directly or indirectly with Mr. Blumenthal; only that he was part of a team being assembled, that they had a contract, that they had a funding vehicle for needed seed money, that they had a Chicago-based law firm and that all members were former USG Intelligence Operations Directorate personnel.

b6  
b7C

[redacted] has a rather controversial history within the US Intelligence Community, particularly at [redacted]. His links to [redacted] was one of the prime operatives in Libya, providing [redacted]. Notwithstanding his reputation in the US Intelligence Community, he was believed to have highly placed contacts within Libya which could have been mined for creation of a Rogue Nation Asset Recovery program, but for his limited technical and intelligence analyst resources.

b6  
b7C

Is it a stretch to believe that at one time or another [redacted] did not stand upon Mr. Blumenthal, Mr. Drumheller and Mr. Murray, who were creating the "shake and bake" SITREPs, and for which he would provide access to the Opposition Government to contract for recovery of the plundered Qaddafi assets? While the time line and the relationship, connections, links and possible association atmospheres do fit; it is still just circumstantial at present.

b6  
b7C

But, so goes the possible theory – If Blumenthal was able to locate and re-patriate the money, it would be a huge win for the US State Department as it could claim they suppressed the money laundering efforts of the Ghaddafi family and repatriated the money to the rightful owners; moreover, saved the American people the cost to fund reconstruction of Libya through this repatriation effort.

However, the legality of such an arrangement, outside of normal US Government channels, authorities and governances is questionable. Such a "quid-pro-quo" would be looked upon from within the Community with great caution and disdain, particularly after it was learned that Blumenthal also had a pecuniary relationship with the Clinton Foundation.

Again, we caution here: We have no definitive evidence that Mr. Blumenthal actually was involved in the above engagement with the Libyan Opposition. All we know for certain is that he was soliciting Senior Intelligence analysts during this period to participate and lend a hand and was doing so using Mr. Murray and Mr. Drumheller.

We know that the Libyan Opposition Government was attempting to contract with intelligence professionals to engage in this program. We also know that they were seeking – through intermediaries – legal counsel who had long experience and achieved some success in rogue national judgment work. And, we know that Mr. Blumenthal was passing to Mrs. Clinton dubious SITREPs that he was characterizing as atmospheric HUMINT reports from alleged intelligence sources in Libya. As stated above, we also know that [redacted] definitely did have a contract with the opposition Government as recently as around 2014, according to his self-confessed claims.

b6  
b7C

Further, we also know that the Libyan Opposition, as recently as December 4<sup>th</sup> 2015 was seeking to re-ignite this program using a man identified as [redacted].<sup>11</sup> Our information suggests that [redacted] was working directly for the new Libyan Foreign minister "on an initiative to locate and freeze Libyan assets that were hidden by Kaddafi around the globe." He also stated "...Until the political situation in Libya becomes stable and a democratic government is elected, all these assets are in danger of being confiscated or misused by politicians or treasure hunters."<sup>12</sup>

b6  
b7C

<sup>11</sup> The email address for [redacted] is identified in [redacted].

b6  
b7C

<sup>12</sup> For additional information on this event, please see [redacted] version of an email dated 4 December 2015 from [redacted] seeking to partner with a local law firm to [redacted]. Document #8 LIBYA ASSET ROGUE NATIONAL JUDGMENT RECOVERY PROGRAM

We note that [REDACTED]

[REDACTED] and as of December 2015 and January 2016, was seeking not only Senior Intelligence analysts, but legal counsel in Washington, DC.

By way of brief background, [REDACTED]

After working for [REDACTED] for several years, [REDACTED] started several private enterprises including [REDACTED]

In addition to operating several businesses in the United States, [REDACTED] also served as a [REDACTED] has served on the board or executive committees of several non-profit and community organizations. Most recently he has been [REDACTED]

[REDACTED] is passionately interested in [REDACTED] and has [REDACTED]

He has strong links to [REDACTED] who lives in [REDACTED]

[REDACTED] has been active in the Libyan revolution since its inception in February 2011. [REDACTED]

[REDACTED] is active in Washington DC's political circles with extensive networks and relationships about Libya and its democratic transition. He frequently participates in programs in prominent think tanks and meets regularly with policy makers and government officials regarding Libya. He maintains strong relationships with important political actors in Libya and continues to advise successive Libyan governments regarding Libya-US relations.

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C



b6  
b7C

Another person linked to both [REDACTED]

b6  
b7C

His business career started in [REDACTED] owned and operated [REDACTED]  
[REDACTED] He also owned and operated [REDACTED] Currently, he owns and  
operates [REDACTED]

b6  
b7C

An active community member [REDACTED] is involved in local and state politics. He is a  
member of various community and political groups and is especially interested in inter-faith  
work. Prior to [REDACTED] was a  
member of [REDACTED] While he resides in [REDACTED]  
maintains an extensive network of contacts in Libya where he travels frequently to meet with  
political leaders and civil society groups.

b6  
b7C

We are not suggesting that any of these men engaged with Mr. Blumenthal. However, what we  
do have proof of is that this group is working directly for the Foreign Minister, and are seeking  
to recruit American Senior Intelligence analysts and legal counsel to contract with the Libyan  
Opposition Government and seek to recover the assets, and did so as recently as 4 December  
2015.

Thus, while there may be circumstantial evidence that a scheme was underway; to this day, there  
is no concrete evidence showing that Mr. Blumenthal actually did achieve a successful *quid pro  
quo* with Mrs. Clinton.

However, at Phase II, we would recommend that it might be worthy to make contact with the  
aforementioned organization and see whether the Libyan Opposition Government ever  
contracted with any groups, organizations or individuals and received reports, memos, work  
product, contracts, corporate vehicles, etc., regarding asset repatriation, without regard to the  
Blumenthal group.

Normally, if [REDACTED] had indeed hired a new group of forensic financial experts or  
Senior Intelligence Analysts, this follow-on organization would ask for copies of all memoranda.  
They would want to have this so not to duplicate past efforts that proved fruitful, or mine the  
data that was recovered for additional leads. If the Libyan Opposition Government did indeed  
contract with Mr. Blumenthal, it is logical that [REDACTED] has the ability to obtain the  
data.

b6  
b7C

### *Example of Data Traced from Hillary Clinton Server Directly to the Deep Web*

While we cannot state for certain at this juncture in the research, that Mrs. Clinton's server was directly penetrated, we did find a sample of a particular document within the Dark Web that traces back to her exact IP address where her domain email server was located. This document is a summary of known and suspected Libyan terrorists who were in and around the Benghazi area.<sup>13</sup> If genuine, this document would enjoy the highest level of classification because it could be used for targeting and would be a record that the Ambassador-in-country would have access to as it was probably obtained by the Chief of Station or an Operations Officer under his authority.

Moreover, this document was not found on Mr. Blumenthal's server so it was not sent by him to anyone and was not received by him from any source.

Rather, it was found in the Deep Web and traced back to Mrs. Clinton's IP only. Therefore, one possible explanation -- using every reasonable inference -- is that it came from Mrs. Clinton and that her server was penetrated. Much more analysis would need to be done on this and other documents that could be recovered to determine when, if and how Mrs. Clinton's server was penetrated and where the documents landed.

### *Use of the Global Scan Search Vehicle to Locate Suspect Document*

Attempting to trace back to the providence of this one document (Attachment #2) and identify all places where it landed, would take some effort. The client may wish to expand the research to include a complete GlobalScan search, which represents the deepest and most in-depth scans that are available in the commercial database world today. Reports can range from 800 to 4000 pages long, when including exhibits.

Global Scan can be done on any person in the world, and costs depend on the name, address, age and other identifiers for the person. To date, we have processed over 20,000 GlobalScans since our inception. After 1996, the GlobalScan always included digital media data, usually from the original source so that they could be used in a legal proceeding.

Since we have much experience in complex digital intelligence research that involves databases and electronic sources, our experience has shown that the only effective way to conduct such a study is the Global Scan® on each person or company or document that we find and trace it back through the movement evolution.

We assume permissible purpose exists for conducting all appropriate database searches. This matter must be confidential and privileged and done pursuant to the privileged communications doctrine and the attorney work-product doctrine.<sup>14</sup>

<sup>13</sup> For additional information on a sample of one file that was recovered from the Deep Web and the Dark Web which came only from Hillary Clinton Server, please see Attachment #2 COPY OF LYBIA ANALYST TRACED TO CLINTON SERVER EMAIL

<sup>14</sup> Please note that some searches require a permissible purpose as defined under the Federal Fair Credit Reporting Act, Title 15, USC 1681, et. seq., as well as other local, state, federal and international laws. You are required to certify to ☐ that any search is in compliance with both FCRA, as well as the 1999 Graham-Leach Bank Privacy Act. By placing any order with ☐ the client represents that the client has fully complied with all local, state, federal and international laws and assumes all responsibility. ☐ assumes no responsibility for determining



However, as stated at the outset, the only exception to the privilege when using Global Scan is if records are found that are demonstrably apparent to be classified, even if not overtly marked as such. If this is found, we must stop, turn over the implicated material to the FBI, and seek their guidance and support.

This search permits us to cite the costs for obtaining all other information within each "information corridor" that may be identified during the initial scan.

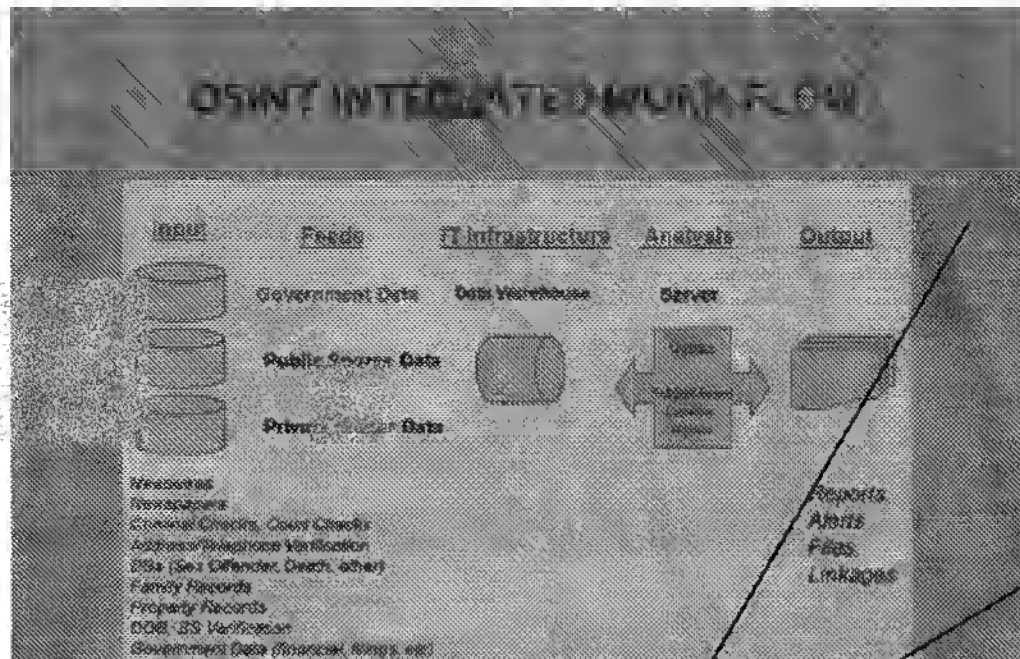
It also enables the ultimate client to maintain control of the scope, direction, and cost of a more extensive investigation. Each proposed search item is listed at the end of initial report.

For example, a Global Scan® will cite the name and address of a bank, an account number, the signatures on the account, and when it was opened, but will not provide information regarding balances or activity. However, the Global Scan® will cite the exact cost for obtaining that next level of information.

Normally, GlobalScan® always includes the following categories of data:

- a. Banking, financial and credit relationships, including addresses and names of institutions.
- b. Real estate holdings, real estate trusts, and real property conveyances.
- c. Corporate affiliations, executive associations, and self-confessed employment.
- d. Credit reports and personal financial scans.
- e. Litigation, including criminal arrests in their areas of residence.
- f. Newspaper, magazine, trade journal, and wire service reports.
- g. Known associates, family members and close personal friends who may be used to transfer or convey assets.
- h. Vehicles, boats, mechanized equipment, and recreational devices traced to merchant's name, address or SSN.
- i. UCC filings recorded in the name of the merchant, based upon a scan of the person's name, SSN, or past addresses, a triple secured search. Included is both debtor and secured party searches.
- j. Identification of trade creditors, credit card companies, utility companies, banks, or other entities that the target would be paying with some type of instrument. These searches do not include identification of the bank that a check is drawn upon, or the account number, just the bill that is being paid.
- k. Identification of telephone numbers, cellular numbers, and mobile telephone numbers; together with long distance carriers. This search does not include a detail of the numbers dialed, or the subscribers to the numbers dialed, which can only be obtained at the next level of searching.
- l. All past addresses, historic use of addresses, names of relatives, names of persons traced to addresses used by the merchant, names of relatives and the statistical identifiers of those that reside in the same household as the merchant.

In actuality, the data flow appears something like that which is depicted below:



Global Scan® is conducted on a flat fee basis only, and is marketed that way because clients seek to have a guaranteed fee structure cited in advance. Moreover, before any Global Scan® can be prepared ☐ requires that all cited fees and expense surcharges be paid in advance.

b6  
b7c

☐ does not bill by the hour for its services nor use "general price lists". Rather, it uses the "bundled billing" approach. In short, the fee is guaranteed and includes all research time, computer data downloads, analysis, report preparation and delivery. We may consult with counsel by telephone or email following transmission of our report, should there be a need to clarify a few points in our report. This approach guarantees the client all available information for a pre-cited charge without regard to the amount of information obtained.

### *Specialized In-Depth Searches*

We also can conduct deeper probes, depending on the requirements of counsel, the permissible purpose to obtain the information, etc. In addition to the above mentioned eight categories of data, we can, under certain circumstances provide a more in-depth report and other kinds of advanced searching. The cost for each depends on the nature of the request. We checked Mr. Blumenthal's digital data and found some or all of these indicators are present:

1. Social Security Numbers and DOB Search
2. Social Security Trace for all addresses, verify date of issuance, state of issuance and whether used regarding banking, financial or credit transaction
3. Date of Birth Records
4. Death Records
5. Change Of Name Records

6. Marriage and divorce Records
7. Criminal Records State or federal sealed or unsealed felony or misdemeanor
8. Warrants of Arrest
9. Order of Protection, domestic violence offender scans
10. Probation Records, special offender searches, including sex offender registries, or habitual offender status
11. Property Tax Records
12. Utility Bill Records
13. Current Address
14. Driver's License Information
15. Car Insurance Records
16. U.S. Postal Service Forwarding Address Records
17. True owner of U.S. Postal Service PO BOX Records
18. Magazines or Newsletters that you are the owner of. (Postal Records)
19. Bulk Mail Permit records (US Postal Service)
20. Magazines that someone may subscribe to
21. Books that are obtained from a library
22. Link State Catalogs register
23. Credit Card Records
24. Credit Records
25. Banking, financial and credit relationships that include name and address of bank
26. MVR Reports
27. TAG & VIN Traces
28. License Plates (Name and address can be found by doing a license plate search)
29. Full Driving Records, including searches of National Major Offender Database
30. Military Records Search, including discharge status, branch job and rating, dates of Enlistment, Reasons for Discharge
31. List of Hospital admissions and possible diagnosis codes
32. Telephone Number Historical Index

33. Cell Phone Trace
34. Unlisted Phone Numbers Decodes
35. Illegal Alien Database Scan
36. Government Job Registration Scan
37. Worker's Compensation Settlement or Claim Scans
38. Automobile and Personal Injury Insurance Fraud Database
39. Real Estate, Co-Op and Full Title Search scan for 50 years
40. Leads for identifying hidden or secret assets that are in the form of T-bills, bonds, stocks, "offshore" bank accounts, or funds in tax haven countries
41. College Records Search, verification of college attendance, degrees conveyed and special awards
42. Terrorist or Cult Member Dossiers
43. Professional Certification by various professional trade associations
44. Business Conduct Searches through databases such as Better Business Bureau
45. Federal Bankruptcy Database Scans, including whether cited in an adversarial proceeding, or as a claimant in any bankruptcy action by others
46. Catalogs, Mailing Lists, and Department Store searches
47. Employment Searches for a period of 20 years, including job titles and descriptions, addresses, and possible level of compensation
48. All Professional Licenses Scan
49. Business licenses, motor vehicle licenses, pilot licenses
50. Evictions and Tenant-Landlord Database Scan
51. Voter Registration Database and scan of historic voting record
52. Email tracing service and complete Web Site Domain.

#### *Understanding Deep Web Intelligence Methodology*

By way of background, the "Deep Web" — a vast reservoir of Internet content that is 500 times larger than known "surface" World Wide Web material. What makes the discovery of the Deep Web so significant is the quality of content found within it. Deep Web searches are intended for cases where historic data needs to be obtained and which otherwise tends to "fall off" current-day data tables.

Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While much can be gathered from the top, there is a wealth of information that lies deeper, and therefore is missed by the average person.

There are hundreds of billions of highly valuable documents hidden in searchable databases that cannot be retrieved by conventional search engines. The reason is simple: basic search methodology and technology has not evolved significantly since the inception of the Internet.

Traditional search engines create their card catalogs by spidering or crawling "surface" Web pages. To be identified, a page must be static and linked to subsequent other pages. Utilized in this manner, standard search engines cannot "see" or retrieve content in the Deep Web and the crawlers used by them cannot probe beneath the surface. The result is that enormous amounts of data remains untapped and effectively "hidden" to the crawler, while in reality, the material is in plain sight.

The discovery of the Deep Web is the result of groundbreaking search technology developed by the Intelligence Community. Private companies have only recently developed search technology capable of identifying, retrieving, qualifying, classifying and organizing "deep" and "surface" content from the World Wide Web.

The Deep Web is qualitatively different from the surface Web. Deep Web sources store their content in searchable databases that only produce results dynamically in response to a direct request. But a direct query is a "one at a time" laborious way to search.

Our search system automates the process of making dozens of direct queries simultaneously using multiple thread technology. It allows searchers to dive deep and explore hidden data simultaneously from multiple sources using directed queries.

Businesses, researchers and consumers now have access to the most valuable and hard-to-find information on the Web and can retrieve it with pinpoint accuracy. If the most coveted commodity of the Information Age is indeed information, then the value of Deep Web content is immeasurable.

When conducting Deep Web intelligence studies on companies or individuals, we access a much different class of documents. Included in the search results are not only the standard information retrieved by conventional search engines but many other possible leads. Some of the highlights of the Deep Web search include:

1. **Public information on the Deep Web that is 400 to 550 times larger than the commonly defined World Wide Web;**
2. **7,500 terabytes of information, compared to 19 terabytes of information in the surface Web;**
3. **550 billion individual documents compared to the 1 billion of the surface Web;**
4. **Information from an additional 100,000 Deep Web sites;**
5. **60 of the largest Deep Web sites collectively contain about 750 terabytes of information — sufficient by themselves to exceed the size of the surface Web by 40 times;**
6. **On average, Deep Web sites receive about 50% greater monthly traffic than surface sites and are more highly linked to than surface sites; however, the typical (median) Deep Web site is not well known to the Internet search public;**

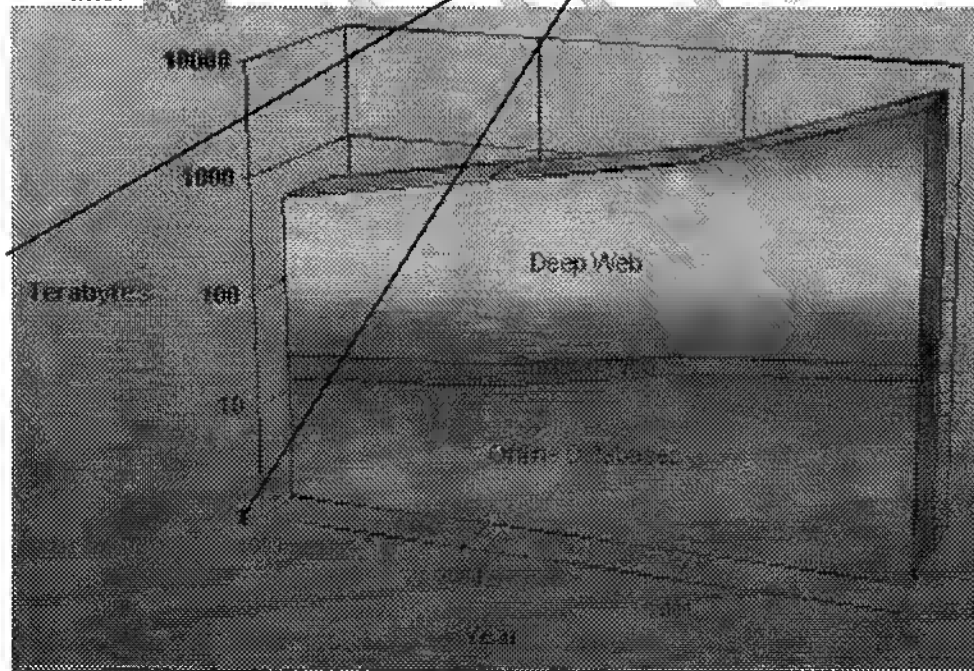
7. The Deep Web is the largest growing category of new information on the Internet;
8. Deep Web sites tend to be narrower with deeper content than conventional surface sites;
9. Total quality content of the deep Web is at least 1,000 to 2,000 times greater than that of the surface Web;
10. Deep Web content is highly relevant to every information need, market and domain. More than half of the deep Web content resides in topic specific databases;
11. A full 95% of the deep Web is publicly accessible information — not subject to fees or subscriptions.

To put these numbers in perspective, we estimate that some of the largest search engines, such as Northern Light, individually index only 16% of the surface Web. Since they are missing the Deep Web, Internet searchers are therefore searching only 0.03% — or one in 3,000 — of the available to them today.

Simultaneous indexing of multiple surface and Deep Web sources is necessary when extensive information retrieval is needed.

the identification of Deep Web sites and the retrieval process for We have also developed a direct-access query engine translatable to already collected, eventually growing to 100,000 sites. It is shown that when the hit scores fall below 65%, they are not deemed reliable and the hits tend to be unrelated to the target of the inquiry.

Graphical comparison of the Deep Web compared to the "surface web" looks something like this:

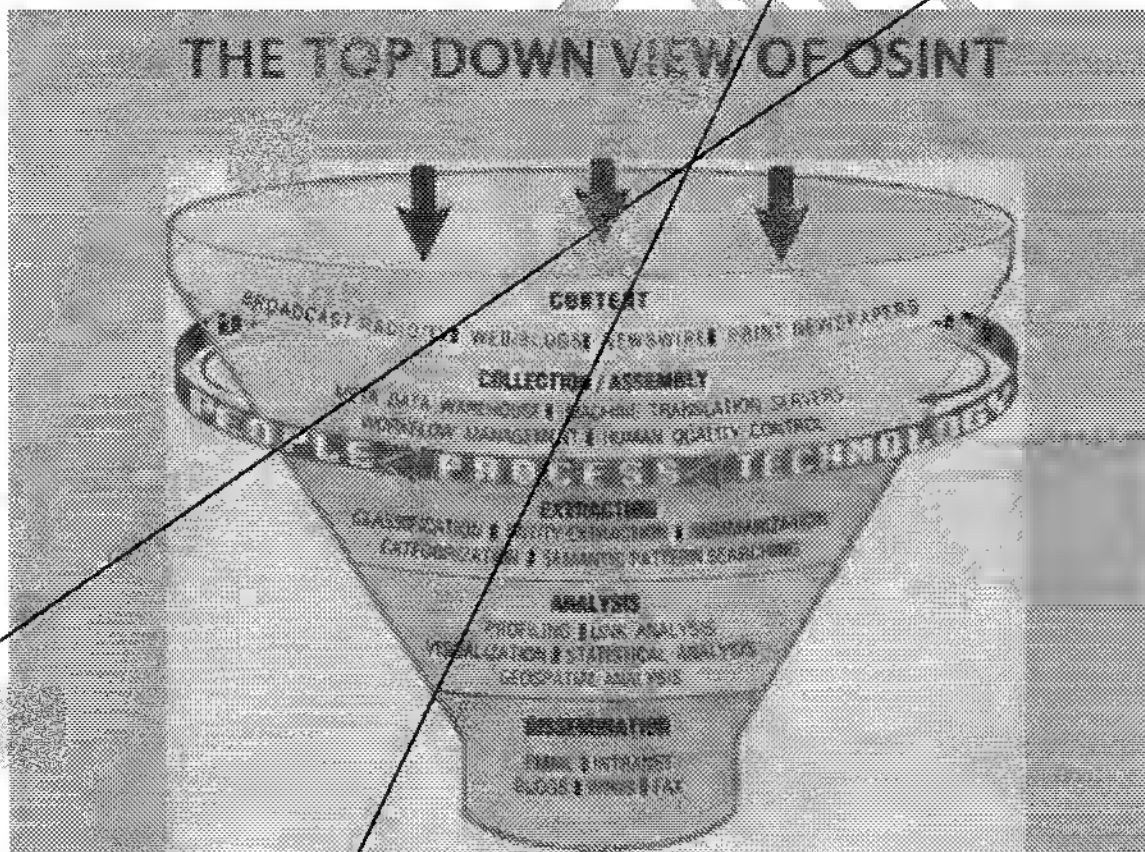


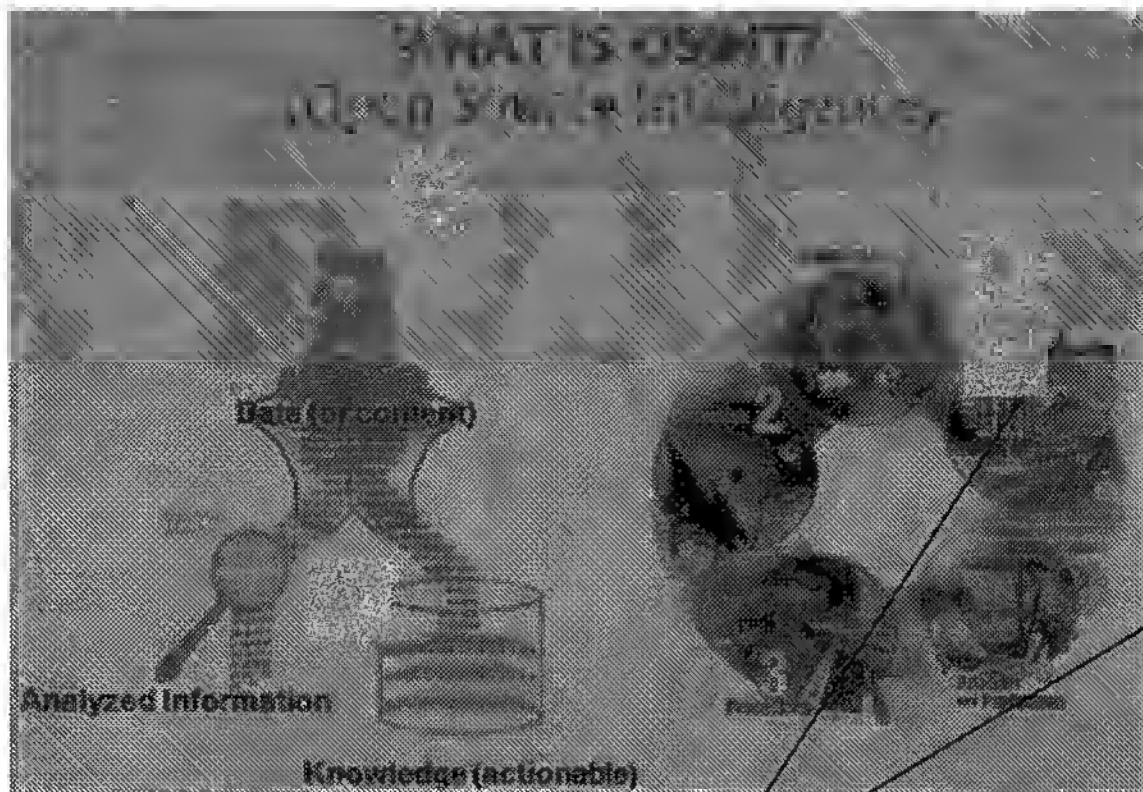


During the past several years, the Department of Defense, led by the Defense Advanced Research Projects Agency (DARPA) has been steadily working on a project called the NOISE database, known as Name Only Index Searching and Exception. The acronym NOISE came from the negative consequence of conventional searching of the Open Source, Web-enabled applications such as:

[www.altavista.com](http://www.altavista.com)  
[www.northernlight.com](http://www.northernlight.com)  
[www.lycos.com](http://www.lycos.com)  
[www.opendirectory.com](http://www.opendirectory.com)  
[www.waybackmachine.org](http://www.waybackmachine.org)  
[www.google.com](http://www.google.com)  
[www.cuil.com](http://www.cuil.com)  
[www.insn.com](http://www.insn.com)

Visually, the process of gathering information on a person or entity looks something like the figure below:





Traditionally, these are "Name Only" or "Business Name only" or "Telephone Number Only" searches that return massive, unrefined results. When the search criteria is common, the return results is often "NOISE" and burdens the analyst with a vast amount of irrelevant information.

In the commercial or legal markets space, the same is true, but the pressure is even greater to obtain results quickly, efficiently, and within a reasonable budget.

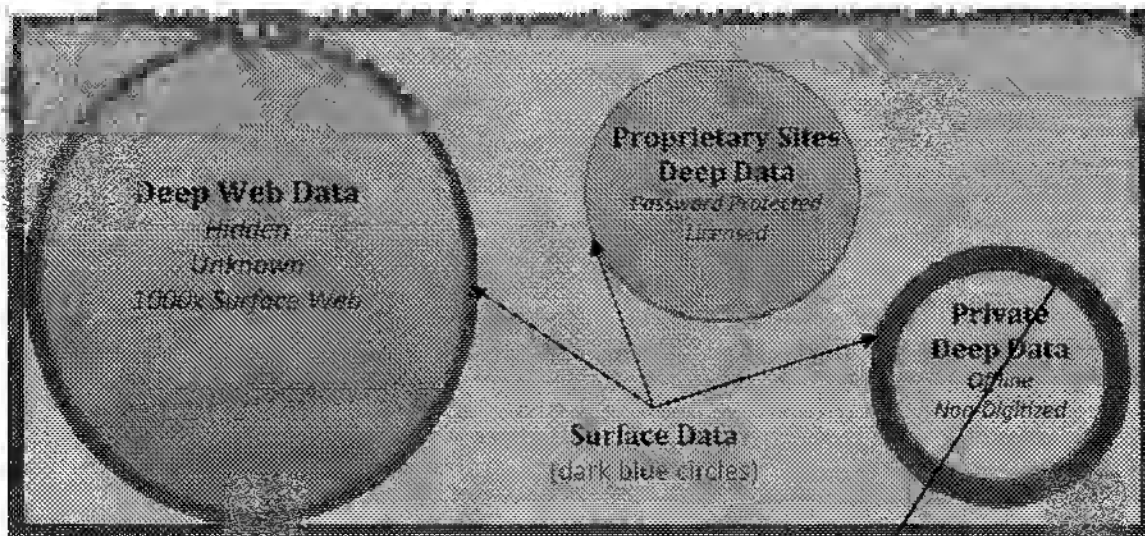
The commercial application of the NOISE application is particularly useful in certain kinds of litigation such as the current Clinton case. It has been used to "walk back" information claimed to be gleaned from foreign IP sources as it can be fished out of the Deep Web and effectively converted for use by analysts.

For that reason, we suggest that NOISE application and the [redacted] data searches be considered here because of the relatively common names of Advantage and the key individuals.

b6  
b7c

It is the union of the NOISE application and the restricted access data within [redacted] that is only available with a permissible purpose that allows for a highly relevant, targeted search approach. It looks something like this:



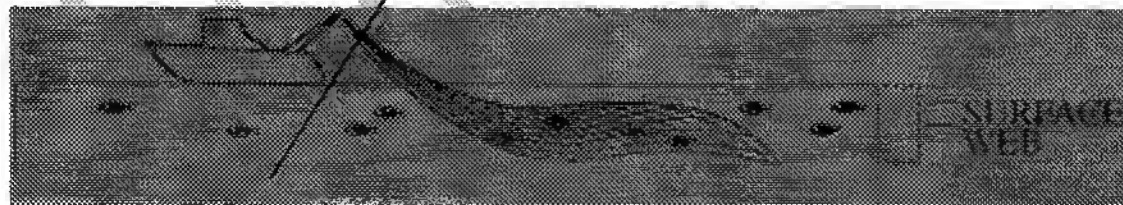


In the DoI, the PA was tasked with the order to find a means to find granular data about (names, dates of birth, ages, past addresses, phone numbers, faxes, email addresses, businesses, names of relatives, etc.) or the so called digital fingerprint of a person and inject that intelligence into the web-enabled application for a more defined search.

For common names, the results are culled down from perhaps 12,000 to 120. Moreover, the data is highly accurate and allows for rifle-shot searching. Because the name *Hillary Clinton* or *Sidney Blumenthal* are so common and lead to millions of stories and hits; this is the perfect tool to cull through the mountains of data that exist on both within the Deep Web.

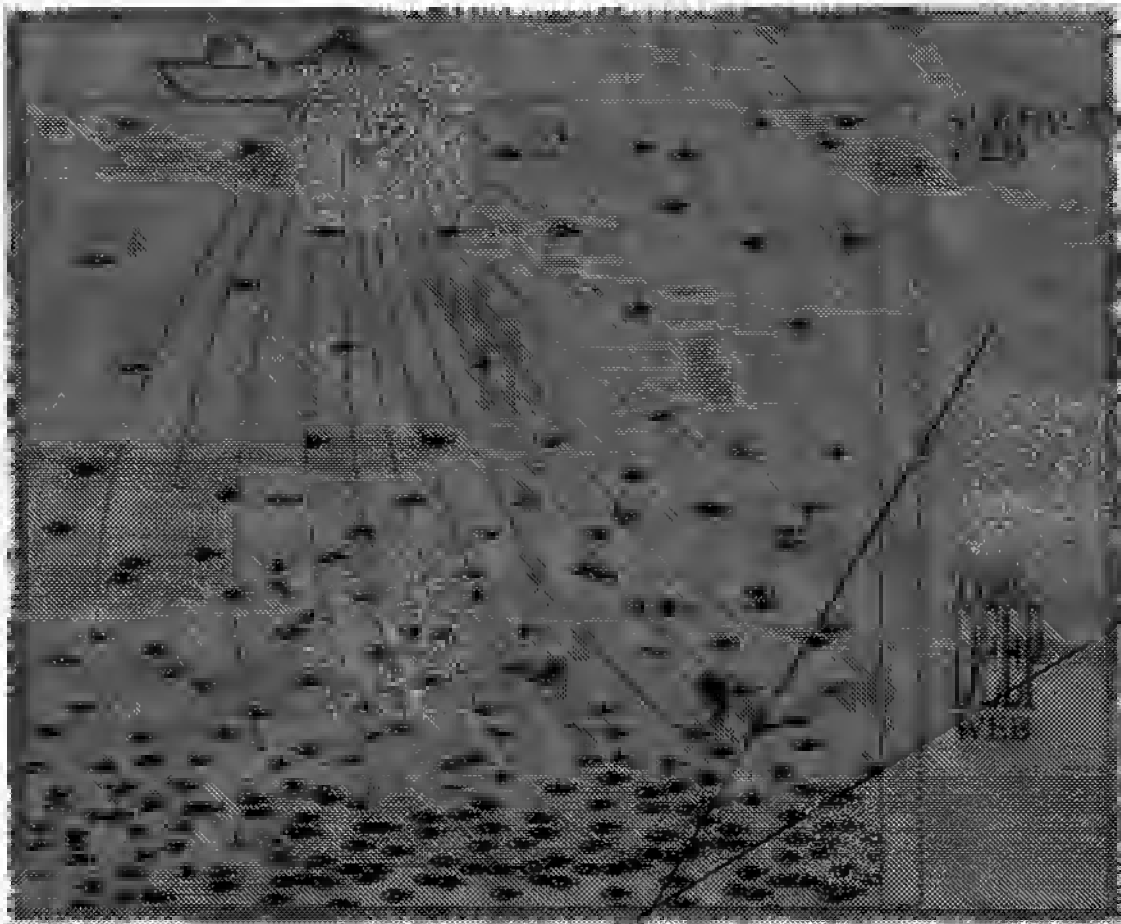
The second compelling reason this new form of search technology was developed is that the Internet and the Deep Web is much larger and vaster than any database source on the planet today. The "Deep Web", sometimes known as the Internet Dark Space or the Deep Web Intelligence Center, is a vast reservoir of content that is 1,000 times larger than the known "surface" World Wide Web. What makes the discovery of the Deep Web so significant is the quality of content found within. In a very real way, the Dark Space of the Internet is much like the outer space: Its depth and size is not measureable, indefinable, and endless.

The old way of searching, looks something like this:



However, the new way, including use of NOISE and  data that can be granularized, looks something like this:

b6  
b7C



This new capability allows searchers to dive deep and explore hidden data from multiple sources simultaneously using directed queries.

When you combine the ability to "Deep Dive" into the Internet, with the ability to access restricted and previously hidden data that is mostly available only to law firms or those with a permissible purpose (DOB, Past Addresses, etc.), one can significantly expand not only the searchable data base but do so with highly accurate results.

Businesses, researchers and consumers now have access to the most valuable and hard-to-find information on the Web and can retrieve it with pinpoint accuracy. Searching on the Internet today can be compared to dragging a net across the surface of the ocean.

However, there is a wealth of information that is deep, and therefore missed, hence, the Deep Web. The reason is simple: basic search methodology and technology have not evolved significantly since the inception of the Internet. Traditional search engines create their card catalogs by spidering or crawling "surface" Web pages.

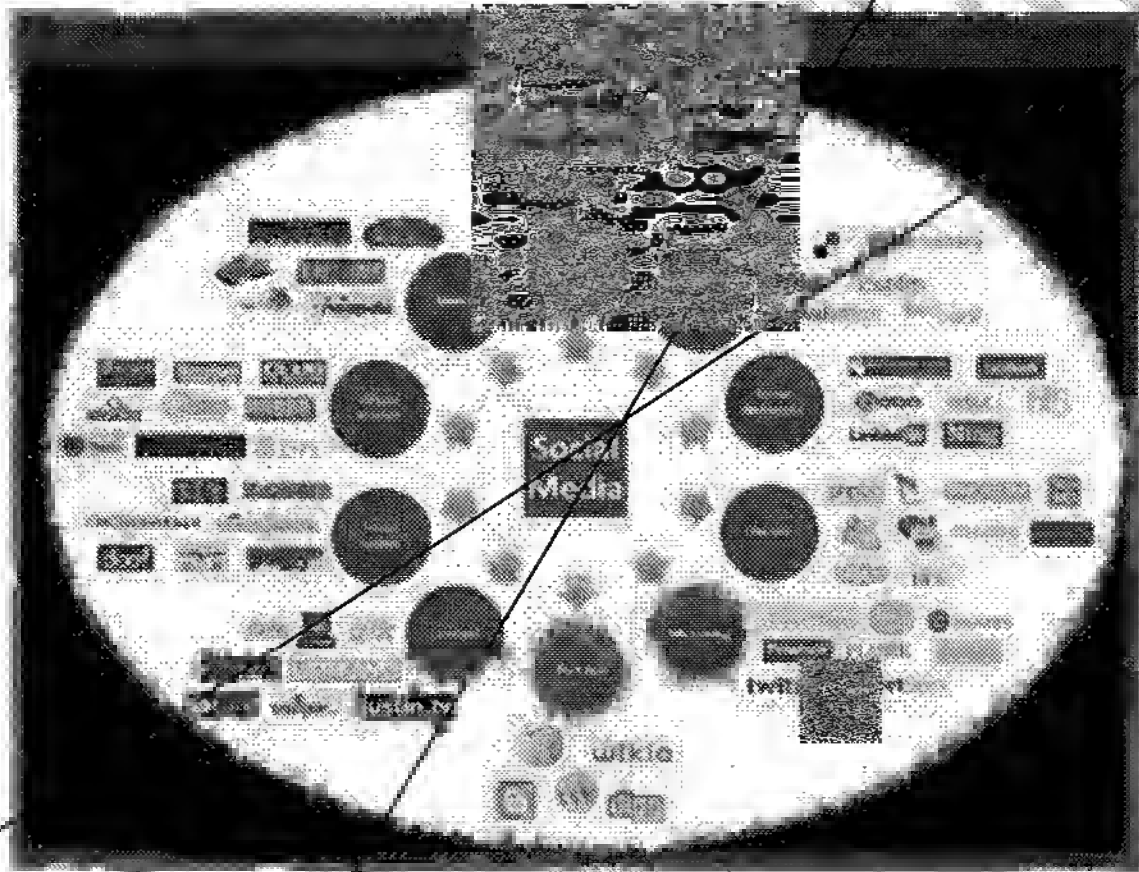
To be discovered, the page must be static and linked to other pages. Traditional search engines cannot "see" or retrieve content in the Deep Web. Because traditional search engine crawlers cannot probe beneath the surface, the Deep Web or Dark Space of the Internet has heretofore been hidden in plain sight.

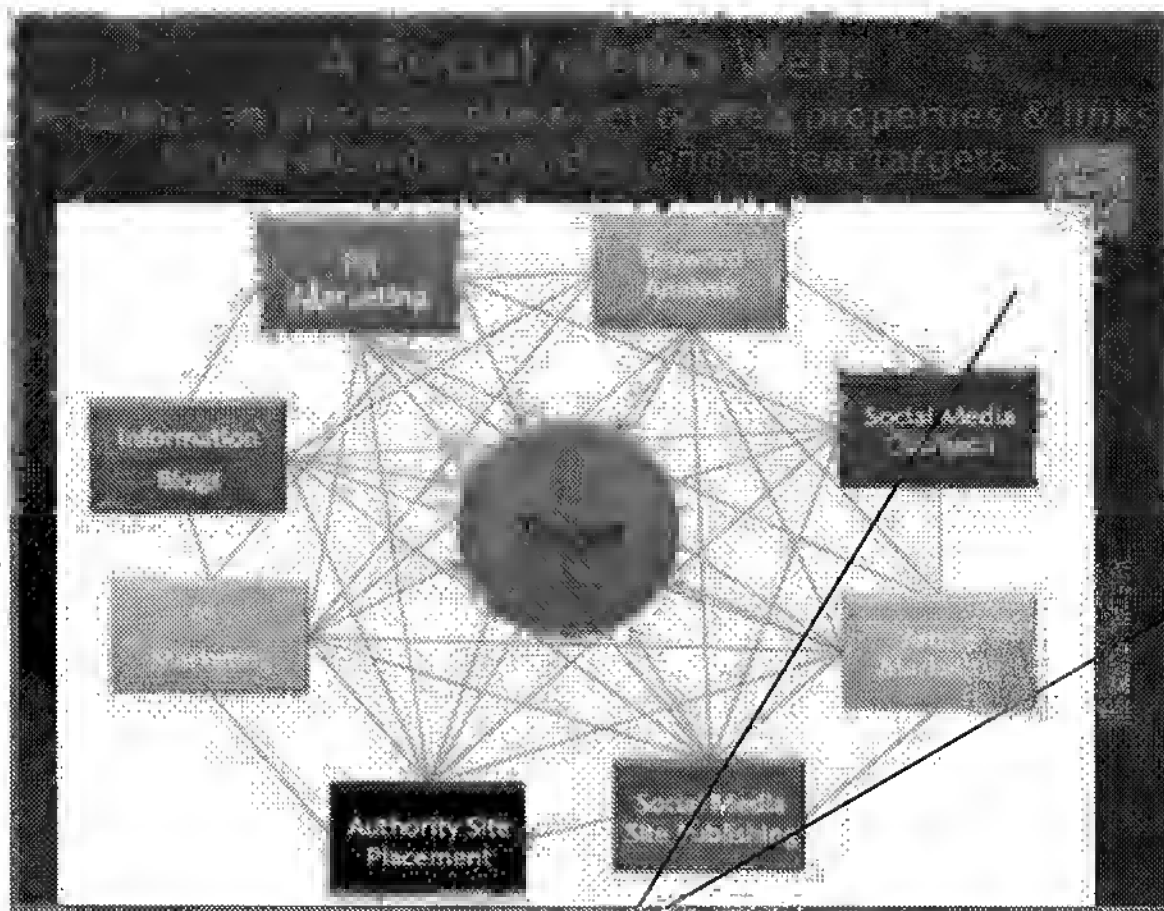
The Deep Web is qualitatively different from the surface Web. Deep Web sources store their content in searchable databases that only produce results dynamically in response to a direct request. But a direct query is a "one at a time" laborious way to search.

NOISE automates the process of making dozens of direct queries simultaneously using multiple thread technology, and takes private, non-public financial information and pulverizes it for inclusion into the search query. If the most coveted commodity of the Information Age is indeed intelligence, then the value of Deep Web content is immeasurable.

Today, more and more people are "self-confessed" habits and haunts; their biases and prejudices and their flavors and peccadillos. It is predominantly done on such Social Media web sites as Facebook, MyLife, LinkedIn, and hundreds of other public and private chat portals. All of these locations are trawled, but the key is the instrument or vehicle used and the advanced analytics applies.

Our technology specializes in the developing of these wide and deep data mining nets and tools, where it is launched upon an endlessly sized ocean of data. Some of these data sources include:





### Summary and Conclusion

The Phase I research confirms that Sidney Blumenthal's server was the target of repeated attacks by *Guccifer* and his colleagues. The penetration resulted in the exfiltration of Hillary Clinton's communications directly from Mr. Blumenthal's server to Bucharest, Romania, where it was placed on a password protected, and encrypted server domain. The data then moved to a second IP address that does not appear to be controlled by *Guccifer*. This is troubling because it demonstrates that data moved outside of the control of *Guccifer* to some unknown third party. It is prima facie evidence of a rolling spill that, at least in part, included data that directly or indirectly originated from the computers or servers of Hillary Clinton and Sidney Blumenthal.

This Romanian domain locality then collected nearly 37,000 files and hosted them for a long period of time, many of which came from a direct attack upon the server of Mr. Blumenthal, but also include direct attacks of others.

One of those persons is believed to be the email domain server of Mrs. Clinton because one document was found on the Romanian domain that traced to the IP address of Mrs. Clinton, and one document was recovered successfully, but many others could exist. We just do not know because in order to definitively determine this, one would need to download all of the 37,000 files, and then open each to see whether any can be directly linked to the Clinton server.

The Clinton security people claim that "security logs of the server show no successful penetrations or attacks." This statement or assessment is without basis in our opinion. In reality, one cannot determine from internal security logs alone whether a sophisticated pernicious attack was executed.

There is a multitude of ways that a penetration and exfiltration can occur and no trace is found within the internal security logs of the targeted server. This includes direct, indirect and collateral attacks upon the email domain server, such as was most likely done here.

It is inescapable that a security breach and a violation of basic server security occurred here, both with Mr. Blumenthal and Mrs. Clinton.

The State Department and the IC basic security protocols regarding email servers for personal use was also systematically violated by Mrs. Clinton. The fact that we found emails regarding attachments that describe the names and identities of targets for attack in Libya that date to about the time of the Benghazi attack is particularly troublesome. Such a document, if authored by a US Government employee who enjoyed original classification authority would enjoy the highest level of classification, most probably Top Secret - SCI and a SAP Code. The fact that this document was found in "the open" and has no security classification collars is highly suspect and deserves critical review and analysis.

In this limited, Phase I inquiry, we cannot determine solely whether Mrs. Clinton's server was directly or indirectly attacked. Its contents could be found within the Deep Web and the Dark Web (c) where records could be obtained (d) and the attack was a pernicious (e) where the records might on a server outside of the US.

Answers to each of these questions, but further studies are recommended to determine whether these records to include original emails can be obtained and recovered, mindful of classification issues and our legal obligations as discussed above.

Separately, we assess that Mr. Blumenthal's true motive for being so aggressive in providing information to Mrs. Clinton regarding Benghazi and Libya was to "bait" her into releasing the State Department intelligence file (a classified record at the SECRET level at a minimum because it came from foreign in-country diplomatic or official sources) that contain a roadmap on how the State Department seized the Qaddafi family assets that had been plundered from the country. The \$30 billion was only a portion of what the coalition government suspect was taken from the Libyan people.

We understand that Mr. Blumenthal presented a proposal to the coalition government that included a team of experts in money laundering and repatriation of absconded assets, but it was wholly dependent upon his ability to obtain quality digital data from disparate sources to fuel the tracing and tracking software. We believe that Mr. Blumenthal team members made clear that he would need:

- (a) The complete financial database image files of the Libyan Central Bank during the Qaddafi years;
- (b) The complete State Department intelligence file containing all information on how they identified, located, and then seized the Qaddafi money;
- (c) The complete Qaddafi CINFIL file to which the State Department would have access;
- (d) Identification of the corporate vehicles created by the Qaddafi family to exfiltrate the funds.



If Mr. Blumenthal were able to obtain all of these records, it would then be possible for the team to perhaps succeed in tracing the funds to their present day location and use a legal team to commence seizure proceedings using the *Moravia Writ* legal method. The potential reward to the Blumenthal team would be tens of millions of dollars, but depended entirely on his ability to leverage his relationship with Mrs. Clinton. The plot was disrupted when the email server, and the memos (samples of which are found at Attachment #5) became p

The bottom line here was "No Data – No Dollars", and without this political quid pro quo, the team's efforts would be doomed.

In addition to the above, the Phase I Study resulted in some other detailed findings that are best summarized below:

1. The computer of Sidney Blumenthal was positively identified as hosting many emails and attachments originating from Hillary Clinton's server and others from the Clinton Foundation. In Phase I, we recovered at least 20 memos from Mr. Blumenthal to Mrs. Clinton that contained Situation Reports (SITREPS) allegedly based upon intelligence sources in Libya.
2. Mr. Blumenthal's server was successfully accessed by Marcel Lazar Lehel, originally from Bucharest, who is also known as *Guccifer* or "Small Fish".
3. While one spreadsheet shows that over 1,000 files were found on a closed encrypted and password protected site of someone other than *Guccifer*, only a full analysis of the spreadsheet will reveal all of the files traced back to Mrs. Clinton's server directly, or to that of Mr. Blumenthal. These files were traced to a computer that was using an application to access the Peer-to-Peer networks. The computer was traced to IP address 84.232.210.154, which points to Bucharest, Romania.
4. One search revealed that data that originated from Mr. Blumenthal's server was transferred to the computer at 84.232.210.154 on July 5, 2009 at 07:12 (Bucharest Time), and yielded many references to "HRC" within the spreadsheet. This data suggests that the content of the computer traced to IP 84.232.210.154, was not *Guccifer*, but someone else who accessed his server. The reason is that this "migration" occurred long after *Guccifer* was identified, arrested, and incarcerated in Romania. Several possible explanations exist: (a) *Guccifer* had a co-conspirator that continued to operate the collection from various sources as a "get out of jail free card"; (b) The computer doing this collecting did belong to *Guccifer*, and he allowed it to run long after he was arrested. This scenario seems unlikely for a number of technical reasons; (c) This computer belongs to a foreign service or someone else who attacked the *Guccifer* server and transferred the data to computer 84.232.210.154.
5. Notwithstanding the above, data from both the Blumenthal computer and the Clinton email server migrated to *Guccifer*, and then to a computer tied to IP 84.232.210.154, both of which were located outside of the United States and outside of the control of the US Intelligence Community. Assuming either contained overtly classified data or retrospectively classified data, this is considered a major Counterintelligence concern and of interest to the Community.
6. *Guccifer* entered the Blumenthal computer several times, first through Blumenthal's AOL account. It is not clear whether *Guccifer* targeted Blumenthal because he represented an opportunity of interest, or because a foreign service directed him to the account. Also, it is not clear whether the account was entered after he first entered the Clinton server or that of someone else on the Clinton domain server.
7. During Phase II, much additional information can be obtained on the sequence, timing and chronology of when the two servers in question were accessed and in what order and how many times.
8. We found indications that *Guccifer* or person or persons acting on his behalf or persons impersonating *Guccifer* did a secondary penetration of Mrs. Clinton's server on May 22, 2009, and other penetrations thereafter.
9. We confirmed that *Guccifer* used an anonymous server located in Russia to conduct the penetration, and therefore, there is a high possibility that the Russian services that monitor these anonymous servers likewise have a copy.

10. One file that was found on Mrs. Clinton's server was not found on the Blumenthal server. This file represents a major loss to the Intelligence Community because it appears to be targeting data. The data is first in Russian and then converted to Arabic. It represents a list of targets that quite possibly was created by a Russian source, located or intercepted by our services, and transmitted to Mrs. Clinton by some unknown person. The file then left her server and was found in the Deep Web and Dark Web.
11. The above cited file, an excel spreadsheet, we assess, would enjoy the highest level of classification if submitted to a person who has original classification authority. The file was found stripped of its collars (if they ever existed). If it is determined by the FBI that this file ever was overtly classified, it will serve as a potential "smoking gun document."
12. *Guccifer* penetrated a number of targets and we recovered over 37,000 files from a computer traced to IP 84.232.210.154 that he obtained. We created a mapping of those files as they appear in the Deep Web. We then tested the spreadsheet and the content behind the spreadsheet (the 37,000 files) using key word fuzzy logic. We confirmed the following Blumenthal memos were found on the Clinton Server and vice versa:

name	Date modified	Type	Size
84.232.210.154\src\memo\33000_0000_0000_0000	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\assad's plans 081812	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\Compton's report on Libya 010413-1	7/5/2014 7:12 AM	Microsoft Word Document	21 KB
84.232.210.154\src\memo\Compton's report on Libya 010412	7/5/2014 7:12 AM	Microsoft Word Document	21 KB
84.232.210.154\src\memo\cure for Ebola 030812	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\George H.W. Bush's election response 030212	7/5/2014 7:12 AM	Microsoft Word Document	26 KB
84.232.210.154\src\memo\intel badge memo re oppression 120412	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\latest French intelligence reports on Algerian hostage crisis 011813	7/5/2014 7:12 AM	Microsoft Word Document	16 KB
84.232.210.154\src\memo\libya Benghazi oil 12/2112	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\src\memo\libya cabinet 100813	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\libya al-Qaeda goes 011513	7/5/2014 7:12 AM	Microsoft Word Document	12 KB
84.232.210.154\src\memo\libya new president 051212	7/5/2014 7:12 AM	Microsoft Word Document	16 KB
84.242.210.154\src\memo\libya leadership private discussions 102513	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\src\memo\magical attack on US in Libya 001212	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\magical German was 1-26-030412	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\magical German was 091312	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\src\memo\magical moves 081412	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\magical private conversation 041412	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\paradise October surprise 111212	7/5/2014 7:12 AM	Microsoft Word Document	12 KB
84.232.210.154\src\memo\paradise October surprise 111212-1	7/5/2014 7:12 AM	Microsoft Word Document	15 KB
84.232.210.154\src\memo\paradise October surprise 100312	7/5/2014 7:12 AM	Microsoft Word Document	14 KB
84.232.210.154\src\memo\paradise October surprise 041313	7/5/2014 7:12 AM	Microsoft Word Document	15 KB

13. A complete copy of the Blumenthal memos sent to Mrs. Clinton were opened recovered in original format and deserves critical analysis by counsel. Most all were word documents and related to a number of issues. These can be provided to counsel as a means to substantiate the claims of *Guccifer*.
14. We did not actually collect the content of Mrs. Clinton's server or the content of computer 84.232.210.154 at Phase I; we merely validated the major premise and hypothesis that data originating from either or both of the Clinton and Blumenthal servers were attacked, directly or indirectly, and then were moved outside of the US to *Guccifer*; and then migrated to computer IP 84.232.210.154, owned and operated by unknown persons. Additional research is required to cut through the 37,000 files found to select those that pertain to Mrs. Clinton and which came directly from her server.
15. We note that there are profound legal questions regarding Phase II because it is not clear what our obligations may be regarding recovery of potentially classified data that may or may not contain actual collars that overtly show the content was classified at the time they were sent to Mrs. Clinton; or emails and attachments that were retrospectively classified but were released in truncated form. Our recovery of such content would be untruncated and in original condition.
16. It is conceivable that one possible motive for Mr. Blumenthal's decision to feed Mrs. Clinton the SITREP reports was to promote his group as a quality private intelligence group in Libya capable of obtaining detailed intelligence from various unnamed, disparate sources as to the thinking, actions, planning and intentions of key operators in the region. We do not opine on the accuracy of the intelligence provided, only the tone and intent of the memos. Our assessment is that they are essentially, crafted as "shake and bake" intelligence assessments, done to promote a need by the Blumenthal group, and not to turnover information because of some legal or moral obligation.

17. There is objective evidence to indicate that a person identified as [redacted] telephone [redacted] (circa 10 January 2012) began to solicit Senior Intelligence Analysts with experience in repatriation of assets plundered by the Qaddafi family. This person began the solicitation process on approximately January 25<sup>th</sup> 2012, claiming that he led was dealing with representatives of a "high level political types in the US within the State Department" and that he personally had high level contacts within the new Libyan Opposition Government that he would have a contract with to begin the repatriation process.
18. [redacted] has a rather controversial history within the US Intelligence Community, particularly at [redacted]. His links to [redacted] was one of the prime operatives in Libya. Notwithstanding his reputation in the US Intelligence Community, he was believed to have highly placed contacts within Libya which could have been mined for creation of a Rogue Nation Asset Recovery program, but for his limited technical and intelligence analyst resources.

b6  
b7C

b6  
b7C

## Phase II

The proposed Phase II study includes:

1. Recovery and sorting of all *Guccifer* data on the server in Romania, to obtain all data that came from Mrs. Clinton's server as well as Mr. Blumenthal's server.
2. Analyze all of the content of the computer IP 84.232.210.154, which appears to be different from the *Guccifer* server, although both apparently are located in the Bucharest, Romania area.
3. *Guccifer* claims in recent reports that the secret server contains about 2 Terabytes of data and represents all of his hacking efforts. We opine this statement is most likely accurate. The spreadsheet that we obtained which maps the secret server substantiates this claim, assuming a portion of it originated from the *Guccifer* server.
4. The Clinton smoking gun data document needs to be mapped back to her server to make the clear connection which has not been satisfactorily established.
5. The IP address and email addresses of Mrs. Clinton and her colleagues who used this server need to be checked to determine whether any content traced back to the server or the email address can be recovered from the Deep Web and the Dark Web sources to which we have access.
6. The recovered data content needs to be date stamped and placed in a chronological are to triangulate against the activities of Mrs. Clinton, particularly around the time when she was dealing with the Benghazi investigation.
7. Counsel needs to determine from quality counsel with National Security experience and intelligence experts, the legal obligations by cleared persons to report and surrender data that may have overtly labeled classified data; or data that would objectively be considered classified had it been hypothetically subjected to a person possessing original classification authority.



FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1353814-0

Total Deleted Page(s) = 3  
Page 11 ~ Duplicate;  
Page 12 ~ Duplicate;  
Page 13 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FD-340 (Rev. 4-11-03)

File Number	302
-------------	-----

b3  
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document 81

Date Received 6-23-2014

From Monica Hanley  
(Name of Interviewee)

Washington (City and State)

**By**

b6  
b7C

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes ☒ No

### Federal Taxpayer Information (FTI)

☐ Yes ☒ No

## Midyear Exam

1A72

Reference: \_\_\_\_\_  
(Communication Enclosing Material)

Description: ☒ Original notes re interview of Monica Hanley  
from 6-23-2016

*disposed.*

**Monica Hanley**

- Why did you create the email archive? SPRING 2013
  - Confirm date of creation [believed to be March 2013. In addition, we see HDR22 accessing mailbox from a Mac from 3/23/13 – 4/1/13.]
  - Why both a laptop computer and a thumb drive?
  - Who instructed who to create it?
  - Who helped her create the archive? Did you work with Bryan Pagliano or Justin Cooper to create the archive? (previously mentioned [redacted] – wrong time frame)
  - Who gave you the login credentials/password for HDR22?
  - Was that the first time you logged in to the mail account? If not, explain.
  - Did anyone else ever log in to her mail account (Huma, etc.)?
  - Did you access the mail using the Macintosh Mail application or via webmail?
  - How did you create the archive? How did you save it (i.e., files on your laptop, thumb drive, CD, kept in the Mail app)? Where did you save it?
  - Did you, or someone else, delete any emails from Clinton's active mailbox after this transfer was completed?
  - Did Clinton change her address from hdr22@clintonemail.com to hrod17@clintonemail.com before OR after the archive was created?
  - Who, if anyone, had access to the laptop until you sent it to PRN?
    - Did anyone request access?
  - After you downloaded the emails to the laptop, did you use the laptop?
  - After you downloaded the emails to the laptop, did you ever access the emails?
- Do you remember [redacted] showing you how to access this archive remotely?
  - What did this archive look like? On what computer did you access this archive?
  - Do you recall the steps? The password/login credentials?
  - Did you provide these credentials to anyone else?
- From where did you purchase Clinton's BlackBerry devices?
- What source document did Clinton use to write her State memoir, *Hard Choices*?

b6  
b7C

b6  
b7C

6/23/2016 Monica Hanley

- March 2013 - created archive
- After BB email hack, conf. call
  - email in one place off server
  - HA, JC,   <sup>maybe</sup> on call (No CM)
  - changing email address
  - HA - choose email address, JC assisted w/ tech transfer
  - advisor - group decision to create
  - JC gave MH laptop, MH took it home
  - Mac Mail (built in application)
  - Remotely log on to server
  - JC walked through steps to transfer
  - <sup>by phone</sup>  
• took day or two
- MH had HRC credentials to check email
  - e.g. HRC looking for old email, MH reforward
  - HRC didn't have pwd - someone would enter on BB
  - HA may have had login creds for HRC
  - If pwd change, BH would tell HA or either JC or BP
- Apple laptop - not Air, Pro (had ethernet port)
  - seemed newer model, silver - created thumb drive archive on computer, too.
- MacBook in one residence, thumb drive in other
  - drive might have been given to HA
  - when MH left office, gave remaining item to HA

b6  
b7C

b6  
b7C

HRC-2228

likely

- Was thumb drive laying around house - didn't purchase
- Intention was to delete off server at house
  - Person likely would have been JC.
- MHA stored in drawer or on desk. in [redacted] b6 b7C  
Apr. No one <sup>else</sup> used computer. Was pwd protected. [redacted]
- HRC changed email <sup>address</sup> after before archive created.
- Sent laptop to [redacted] in 2014 b6 b7C
- Tried to send email remotely - didn't work, so sent to [redacted] 10/9/2013
- Was at HRC residence, used laptop to connect to HRC WiFi in Chap., NY. [redacted] tried to remote in, but didn't work. b6 b7C
- BB purchase - AT&T store in Dufont, Amazon (after state) [redacted] someone in Pres. Clinton's office had AT&T contact, another from Pentagon City AT&T store. eBay or.
- HRC would ask MHA to print chapters as wrote memoir
- No knowledge of authors having email.
- Multi hour meetings, HRC would talk about material from book
- Sent MacBook to [redacted] b6 b7C

→ <https://broker.gotoassist.com>

Monica Hanley

After Sid Attack - but who's idea?

- Why did you create the email archive? SPRING 2013
  - Confirm date of creation [believed to be March 2013. In addition, we see HDR22 accessing mailbox from a Mac from 3/23/13 - 4/1/13.]
  - Why both a laptop computer and a thumb drive?
  - Who instructed who to create it?
  - Who helped her create the archive? Did you work with Bryan Pagliano or Justin Cooper to create the archive? [previously mentioned [redacted] - wrong time frame]
  - Who gave you the login credentials/password for HDR22? i.e. How did you access the account?
  - Was that the first time you logged in to the mail account? If not, explain.
  - Did anyone else ever log in to her mail account (Huma, etc.)?
  - Did you access the mail using the Macintosh Mail application or via webmail?
  - How did you create the archive? How did you save it (i.e., files on your laptop, thumb drive, CD, kept in the Mail app)? Where did you save it?
  - Did you, or someone else, delete any emails from Clinton's active mailbox after this transfer was completed?
  - Did Clinton change her address from hdr22@clintonemail.com to hrod17@clintonemail.com before OR after the archive was created? *email changed before archive.*
  - Who, if anyone, had access to the laptop until you sent it to PRN? *Where was it stored in the apt?*
    - Did anyone request access?
  - After you downloaded the emails to the laptop, did you use the laptop? *Secured?*
  - After you downloaded the emails to the laptop, did you ever access the emails?
- Do you remember [redacted] showing you how to access this archive remotely? [redacted] *@ PRN*
  - What did this archive look like? On what computer did you access this archive?
  - Do you recall the steps? The password/login credentials?
  - Did you provide these credentials to anyone else?

b6  
b7C

b6  
b7C

b6  
b7C

- From where did you purchase Clinton's BlackBerry devices? *Aftermarket?*
- What source document did Clinton use to write her State memoir, *Hard Choices*?

*Pretty sure they didn't have access to emails  
started w/ long mtgs where she would talk about.*

HRC-2230

https://broker.gotassist.com/h/  
CITN x assist? Question = 6051-  
438-752

10-9-13

After S.B Hack - changing email address

Implementer - not decision maker

HA, JC, [ ] (not entirely sure) → advisor after

↓ → assisted in transfer of info.  
decided on email

b6  
b7C

b6  
b7C

Drove to NY from [ ]  
got laptop from JC.

never wrote down pswd

MacMail - built in mail application

log on remotely to server.

Did have Pswd.  
Sometimes checked  
account.

to pull up.

range of Pswd.  
HA - inform

HRC -

Justin & Brian

Mac - not air

Computer - data port - probably pro and ethernet  
port - newer model. looked never used.  
think silver.

Thumbdrive - 1 res.

Macbook - 1 res.

Initial goal to get into from laptop  
to server

tried to send remotely but didn't work.

NY Residence

website

BB.

ATT Store - Dupont

Ebay /  
1 x @ Amazon - after DoS

[ ] Je asst.  
1 x Pres Clinton's Staff

liaison from NY AT&T

b6  
b7C

Pentagon Call.

HRC-2234

2-11-14



password# or #password.



#74

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

302

b3  
b7E

Field Office Acquiring Evidence

WF

Serial # of Originating Document

89

Date Received

7-1-2016

From

[Redacted]

Monica Hanley

(Contributor/Interviewee)

b6  
b7C

(Address)

(City and State)

By

[Redacted]

b6  
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)  
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A74

Midyear Exam

Reference:

Emails between Hanley & [Redacted]

(Communication Enclosing Material)

b6  
b7C

Description:

☐ Original notes re interview of

Emails between Hanley & [Redacted]

b6  
b7C

HRC-2240

[REDACTED] WF) (FBI)

b6  
b7C

**From:** [REDACTED]  
**Sent:** Friday, July 01, 2016 1:04 PM  
**To:** [REDACTED] WF) (FBI)  
**Cc:** [REDACTED]  
**Subject:** Hanley [REDACTED] emails  
**Attachments:** Hanley [REDACTED] Email 2.10.2014.pdf; Hanley [REDACTED] Email 2.11.2014.pdf; Hanley-  
[REDACTED] Email 9.23.2013.pdf; Hanley [REDACTED] Email 10.7.2013.pdf; Hanley [REDACTED]  
Email 10.9.2013.pdf; Hanley [REDACTED] Email 10.16.2013.pdf

Dear Special Agent [REDACTED] as requested, attached are copies of Ms. Hanley's email communications with [REDACTED]  
[REDACTED] related to the laptop/email archive matter. Please let us know if there is anything else you require. I  
apologize for the delay in sending this, but I was out of town earlier this week and just returned today. [REDACTED]

b6  
b7C

[REDACTED]  
[REDACTED]  
[REDACTED] Washington, DC 20001-4412 [REDACTED]  
[REDACTED] TEL [REDACTED]  
[REDACTED]

b6  
b7C

[Download V-Card](#) | [View Biography](#)

CONFIDENTIALITY WARNING: This email may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe that you have received this email in error, please notify the sender immediately and delete it from your system.



Monica Hanley [redacted]

b6  
b7C**HRC emails**

20 messages

Monica Hanley [redacted]

Mon, Feb 10, 2014 at 8:55 PM

b6  
b7C

To: [redacted]  
Cc: [redacted]@gmail.com>

Hi [redacted]

I am no longer with HRC's office [redacted] but I wanted to try to finish the HRC email project which requires sending all of her archived email to your server. You recall that we couldn't figure out a way for you to connect to the laptop that I have in my possession.

Do you have time to try tomorrow? Last time, I tried from HRC's home but tomorrow I can try from my home, which has good wifi.

I'm adding [redacted] for her situational awareness. [redacted] as soon we've transferred the email, I'll figure out a way to get the wiped laptop to you.

best,  
Monica

[redacted]

[redacted]  
To: Monica Hanley [redacted]  
Cc: [redacted]@gmail.com>

Mon, Feb 10, 2014 at 9:02 PM

b6  
b7C

Hi [redacted]

I should be able to work with you on this tomorrow morning, can we shoot for around 11a EST?

From: Monica Hanley [mailto:[redacted]]  
Sent: Monday, February 10, 2014 8:55 PM  
To: [redacted]  
Cc: [redacted]  
Subject: HRC emails

b6  
b7C

[Quoted text hidden]

This email has been scanned for email related threats and delivered safely by Mimecast.

For more information please visit <http://www.mimecast.com>

---

Monica Hanley [redacted]  
To: [redacted]  
Cc: [redacted]@gmail.com>

Mon, Feb 10, 2014 at 9:03 PM

b6  
b7C

sounds great  
if tomorrow falls through for you, we can find another time. Will email you in the morning.  
[Quoted text hidden]

---

Monica Hanley [redacted]  
To: [redacted]  
does this morning still work for you?  
[Quoted text hidden]

Tue, Feb 11, 2014 at 11:00 AM

b6  
b7C

---

[redacted]  
To: Monica Hanley [redacted]

Tue, Feb 11, 2014 at 11:08 AM

b6  
b7C

Sure thing

Can you fire up the Mac that has the emails on it, and go to this address from that Mac?

<https://broker.gotoassist.com/h/citrixassist?Question=DP07-267-592>

---

From: Monica Hanley [mailto:[redacted]]  
Sent: Tuesday, February 11, 2014 11:00 AM  
To: [redacted]  
Subject: Re: HRC emails

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

---

Monica Hanley [redacted]  
To: [redacted]

Tue, Feb 11, 2014 at 11:11 AM

b6  
b7C

done. let me know if you can see the screen  
[Quoted text hidden]

---

Tue, Feb 11, 2014 at 11:11 AM

b6  
b7C

To: Monica Hanley [redacted]

b6  
b7C

Monica, I can see your screen now. Can you call me real quick? [redacted]

**From:** Monica Hanley [mailto:[redacted]]

**Sent:** Tuesday, February 11, 2014 11:00 AM

**To:** [redacted]

**Subject:** Re: HRC emails

b6  
b7C

does this morning still work for you?

[Quoted text hidden]

[Quoted text hidden]

---

**Monica Hanley** [redacted]

**To:** [redacted]  
[redacted]  
[redacted]

[Quoted text hidden]

Tue, Feb 11, 2014 at 11:18 AM

b6  
b7C

---

**To:** Monica Hanley [redacted]

Tue, Feb 11, 2014 at 12:28 PM

b6  
b7C

Monica, my remote session disappeared, maybe the laptop went into sleep mode?

**From:** Monica Hanley [mailto:[redacted]]

**Sent:** Tuesday, February 11, 2014 11:18 AM

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

b6  
b7C

---

**mon** [redacted]

**To:** [redacted]

Tue, Feb 11, 2014 at 12:34 PM

b6  
b7C

will check I'm out but headed back to the apt now

[Quoted text hidden]

---

**To:** mon [redacted]

Tue, Feb 11, 2014 at 12:34 PM

b6  
b7C

No worries, let me know when you can get back over there to power it up

**From:** mon [mailto:[REDACTED]]  
**Sent:** Tuesday, February 11, 2014 12:34 PM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

---

**Monica Hanley** [mailto:[REDACTED]]  
**To:** [REDACTED]

Tue, Feb 11, 2014 at 12:56 PM

b6  
b7C

i'm home now  
should i click on the same link that you sent this morning?

[Quoted text hidden]

---

[REDACTED]  
**To:** Monica Hanley [mailto:[REDACTED]]

Tue, Feb 11, 2014 at 12:59 PM

b6  
b7C

I'll have to send you a new one, standby

**From:** Monica Hanley [mailto:[REDACTED]]  
**Sent:** Tuesday, February 11, 2014 12:57 PM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

---

[REDACTED]  
**To:** Monica Hanley [mailto:[REDACTED]]

Tue, Feb 11, 2014 at 12:59 PM

b6  
b7C

<https://broker.gotoassist.com/h/citrixassist?Question=DR960-073-880>

**From:** Monica Hanley [mailto:[REDACTED]]  
**Sent:** Tuesday, February 11, 2014 12:57 PM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

---

[REDACTED]  
**To:** Monica Hanley [mailto:[REDACTED]]

Tue, Feb 11, 2014 at 1:03 PM

b6  
b7C

I am back in, thanks.

I am still having problems connecting to the server. I am enlisting [redacted] help since he has a similar setup, he should be sending me some screenshots soon

b6  
b7C

**From:** Monica Hanley [mailto:[redacted]]  
**Sent:** Tuesday, February 11, 2014 12:57 PM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

---

[redacted]@gmail.com>  
**To:** Monica Hanley [redacted]  
**Cc:** [redacted]

Tue, Mar 25, 2014 at 4:42 PM

b6  
b7C

Hi guys - just following up on this. Let me know when the wiped laptop is ready to be shipped. [redacted] best to send it to the foundation at:

Hillary Rodham Clinton  
c/o [redacted]  
1271 Avenue of the Americas  
42nd Floor  
New York, NY 10020

Let me know once it's gone out so we know to expect it. Thanks [redacted]

---

[redacted] on, Feb 10, 2014 at 9:03 PM, Monica Hanley [redacted] wrote:  
[redacted] text hidden]

b6  
b7C

---

[redacted]@gmail.com>  
**To:** Monica Hanley [redacted]  
**Cc:** [redacted]

Fri, Apr 4, 2014 at 10:09 AM

b6  
b7C

Just checking back on this. [redacted] is it still with you? Thank you [redacted]

[Quoted text hidden]

---

[redacted]  
**To:** [redacted]@gmail.com>, Monica Hanley [redacted]

Fri, Apr 4, 2014 at 10:11 AM

b6  
b7C

Sorry, missed this the first time around. Yes, the email has been imported into an archive mailbox on the server, and I can send the mac back to you soon

**From:** [redacted]@gmail.com]

b6  
b7C

**Sent:** Friday, April 04, 2014 10:10 AM

**To:** Monica Hanley

**Cc:** [REDACTED]

**Subject:** Re: HRC emails

b6  
b7C

Just checking back on this [REDACTED] is it still with you? Thank you [REDACTED]

[Quoted text hidden]

[Quoted text hidden]

---

**Monica Hanley** [REDACTED]  
**To:** [REDACTED]  
**Cc:** [REDACTED]@gmail.com>

Sat, Apr 5, 2014 at 11:54 AM

b6  
b7C

I know I don't work with you anymore so no need to reply to me but if HRC wants access to her email, can she now access it through the web? [REDACTED] I think you should update Huma and [REDACTED] on where all of her old email is.

[Quoted text hidden]

---

[REDACTED]@gmail.com>  
**To:** Monica Hanley [REDACTED]  
**Cc:** [REDACTED]

Sat, Apr 5, 2014 at 1:55 PM

b6  
b7C

makes sense! would love the details - thanks!

[Quoted text hidden]





Monica Hanley [redacted]

b6  
b7C

[redacted] address

5 messages

Tue, Feb 11, 2014 at 3:23 PM

b6  
b7C

To: "Monica Hanley" [redacted]

Here's my home address where I work from:



This email has been scanned for email related threats and delivered safely by Mimecast.  
For more information please visit <http://www.mimecast.com>

mon [redacted]

Mon, Feb 24, 2014 at 11:29 AM

b6  
b7C

To: [redacted]

finally sent this out so u will receive tomorrow.  
tracking number is 8046 1373 3770  
pw is either [redacted]

let me know if you need anything and thanks!  
(Quoted text hidden)

Mon, Feb 24, 2014 at 11:40 AM

b6  
b7C

to: mon [redacted]

Thanks!

From: mon [mailto:[redacted]]  
Sent: Monday, February 24, 2014 11:29 AM

b6  
b7C

To: [redacted]  
Subject: Re: [redacted] address

[Quoted text hidden]

[Quoted text hidden]

---

Tue, Feb 25, 2014 at 1:22 PM

To: mor [redacted]

b6  
b7C

Monica, I received the laptop, I will put some time on my calendar this week to get the email exported and put onto the server. Best of luck in your next job!

---

From: mon [mailto:[redacted]]

Sent: Monday, February 24, 2014 11:29 AM

To: [redacted]

Subject: Re: [redacted] address

b6  
b7C

finally sent this out so u will receive tomorrow.

[Quoted text hidden]

[Quoted text hidden]

---

mon [redacted]

To: [redacted]

Tue, Feb 25, 2014 at 2:02 PM

b6  
b7C

terrific. thank you!

[Quoted text hidden]



Monica Hanley [redacted]

b6  
b7C**HRC - time sensitive**

3 messages

Mon [redacted] Mon, Sep 23, 2013 at 8:14 PM  
Reply-To: [redacted]  
To: [redacted]

b6  
b7C

H [redacted] its monica w HRC. Her berry got creamed. I'm on my way out to buy a berry for her but are you avail to help with the enterprise activation tonight? Pls let me know [redacted] is my cell.

Monica Hanley [redacted] Thu, Oct 3, 2013 at 4:35 PM  
To: [redacted]

b6  
b7C

hi [redacted] so we are going for the transfer tomorrow  
pw for enterprise activation is still the same as you told me on the phone?  
[Quoted text hidden]

[redacted] Thu, Oct 3, 2013 at 4:37 PM  
To: Monica Hanley [redacted]

b6  
b7C

I will set it again- It clears after each activation. It will be [redacted] again.

I'll be around tomorrow if you run into any problems

From: Monica Hanley [mailto:[redacted]]  
Sent: Thursday, October 03, 2013 4:35 PM  
To: [redacted]  
Subject: Re: HRC - time sensitive

b6  
b7C

[Quoted text hidden]



Monica Hanley [redacted]

b6  
b7C**HRC BB**

9 messages

To: Monica Hanley [redacted]

Mon, Oct 7, 2013 at 11:38 AM

b6  
b7C

Hi Monica-

I take it everything went fine with HRC's new blackberry, since we didn't receive any calls/emails from you. Let me know if otherwise J

[redacted]  
b6 Per FBI, DOS  
b7C

Mon [redacted]

Wed, Oct 9, 2013 at 9:52 AM

Reply-To [redacted]

To [redacted]

Hi [redacted]

Yes the enterprise activation went off without a hitch [redacted] did the switch.

There are a couple of preference and apps that [redacted] can't figure out how to download (like a google search app) but I'll take a stab at it when I see her on sunday.

I have the laptop today and good wifi if you have time to do the email switchy-transfer thing today.

**From** [redacted]**Date:** Mon, 7 Oct 2013 15:38:47 +0000**To:** Monica Hanley [redacted]**Subject:** HRC BBb6  
b7C

Hi Monica-

I take it everything went fine with HRC's new blackberry, since we didn't receive any calls/emails from you. Let me know if otherwise J

[redacted]  
Wed, Oct 9, 2013 at 9:54 AMb6  
b7C

I'd like to set up a remote control session on the Mac- what email address would be best to send the link to, for

you to get it on the archive laptop ?

---

**From:** Mon [mailto:[REDACTED]]  
**Sent:** Wednesday, October 09, 2013 9:53 AM  
**To:** [REDACTED]  
**Subject:** Re: HRC BB

[Quoted text hidden]

b6  
b7C

---

**Mon** [REDACTED] **Wed, Oct 9, 2013 at 9:56 AM**  
**Reply-To:** [REDACTED]  
**To:** [REDACTED]

b6  
b7C

This one [REDACTED]  
Also, can we reset HRC's password at some point today?

---

**From:** [REDACTED]  
**Date:** Wed, 9 Oct 2013 13:54:25 +0000  
**To:** [REDACTED]  
**Subject:** RE: HRC BB

b6  
b7C

[Quoted text hidden]

---

[REDACTED] **Wed, Oct 9, 2013 at 9:59 AM**  
**To:** [REDACTED]

b6  
b7C

We can reset HRC's password anytime you'd like. You can either tell me what to set it to, or the more secure option would be to login to webmail, then click Options > Change password in the upper right corner of the webmail interface. Let me know if you need any help with that.

Here's the remote control code for the archive laptop, please fire this up from the laptop and accept any prompts to open/run/download/etc and we should get hooked up. The code is only good for 30 min, so if you're busy and we need to delay this a bit, let me know when you're ready and I can generate a new one.

<https://broker.gotoassist.com/h/citrixassist?Question=DR988-932-848>

[REDACTED]

---

**From:** Mon [mailto:[REDACTED]]  
**Sent:** Wednesday, October 09, 2013 9:57 AM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

Mon [redacted]  
Reply-To: [redacted]  
To: [redacted]

Wed, Oct 9, 2013 at 10:00 AM

b6  
b7C

Yes sorry won't be by wifi until 11am. Is that ok?

From: [redacted]  
Date: Wed, 9 Oct 2013 13:59:40 +0000  
[Quoted text hidden]

b6  
b7C

[redacted]  
To: [redacted]

Wed, Oct 9, 2013 at 10:03 AM

b6  
b7C

Totally fine, send me another email when you're good to go

From: Mon [mailto:[redacted]]  
Sent: Wednesday, October 09, 2013 10:01 AM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]

Monica Hanley [redacted]  
To: [redacted]

Wed, Oct 9, 2013 at 11:15 AM

b6  
b7C

ready!

[Quoted text hidden]

[redacted]  
To: Monica Hanley [redacted]

Wed, Oct 9, 2013 at 11:17 AM

b6  
b7C

Here you go: <https://broker.gotoassist.com/h/citrixassist?Question=DR963-617-436>

From: Monica Hanley [mailto:[redacted]]  
Sent: Wednesday, October 09, 2013 11:16 AM

b6  
b7C

[Quoted text hidden]

[Quoted text hidden]



Monica Hanley [redacted]

b6  
b7C

---

**Remote link**

1 message

---

To: Monica Hanley [redacted]

Wed, Oct 9, 2013 at 11:40 AM

b6  
b7C

<https://broker.gotoassist.com/h/citrixassist?Question=DR051436752>



Monica Hanley [redacted]

b6  
b7C**Computer**

8 messages

**Huma Abedin** <Huma@clintonemail.com>

Wed, Oct 16, 2013 at 9:01 AM

To: [redacted]

b6  
b7C

I cannot get into my outlook.

Keeps saying my name or pw isn't correct. Did they do something to our system?

**Monica Hanley** [redacted]

Wed, Oct 16, 2013 at 9:11 AM

To: Huma Abedin &lt;Huma@clintonemail.com&gt; [redacted]

b6  
b7C

not that i know of.

Did you use this website?

<https://mail.clintonemail.com/owa>

Adding [redacted] to confirm.

[Quoted text hidden]

Wed, Oct 16, 2013 at 9:20 AM

To: Monica Hanley [redacted] Huma Abedin &lt;Huma@clintonemail.com&gt;

b6  
b7C

Hi Huma- Please let me know what method you are using to access your email (web, Outlook, mobile device, etc). Also please try your username/password on the site below from Monica. I can reset your password if necessary.

**From:** Monica Hanley [mailto:[redacted]]**Sent:** Wednesday, October 16, 2013 7:12 AM**To:** Huma Abedin; [redacted]**Subject:** Re: Computerb6  
b7C

[Quoted text hidden]

**Huma Abedin** <Huma@clintonemail.com>

Wed, Oct 16, 2013 at 9:31 AM

To: [redacted]

b6  
b7C

On the web using that site below.

Keep getting same message

**From:** [redacted] [mailto:[redacted]]**Sent:** Wednesday, October 16, 2013 09:20 AM Eastern Standard Timeb6  
b7C



**To:** 'Monica Hanley' [redacted] Huma Abedin  
**Subject:** RE: Computer

b6  
b7C

[Quoted text hidden]

---

Wed, Oct 16, 2013 at 9:41 AM

b6  
b7C

To: Huma Abedin <Huma@clintonemail.com> [redacted]

Huma- I have set your password to not expire, please try again. If it still gives the same message, I will reset your password and you can change it to whatever you'd like

---

**From:** Huma Abedin [mailto:Huma@clintonemail.com]  
**Sent:** Wednesday, October 16, 2013 7:31 AM  
**To:** [redacted]  
**Subject:** Re: Computer

b6  
b7C

[Quoted text hidden]

---

Wed, Oct 16, 2013 at 9:42 AM

b6  
b7C

**Huma Abedin** <Huma@clintonemail.com>  
**To:** [redacted]

SUCCESS

thank you!

---

**From:** [redacted]  
**Sent:** Wednesday, October 16, 2013 9:41 AM  
**To:** Huma Abedin; [redacted]  
**Subject:** RE: Computer

b6  
b7C

[Quoted text hidden]

---

Wed, Oct 16, 2013 at 9:41 AM

b6  
b7C

**Huma Abedin** <Huma@clintonemail.com>  
**To:** [redacted]

Not sure what you did but it works after 35 times of trying!

---

**From:** Huma Abedin  
**Sent:** Wednesday, October 16, 2013 09:31 AM Eastern Standard Time  
**To:** [redacted]  
**Subject:** Re: Computer

b6  
b7C

[Quoted text hidden]

[REDACTED] Wed, Oct 16, 2013 at 9:42 AM

b6  
b7C

To: Huma Abedin <Huma@clintonemail.com> [REDACTED]

Great! I set your password to not expire, I think it had just run out of time. It won't do so again

---

**From:** Huma Abedin [mailto:Huma@clintonemail.com]

**Sent:** Wednesday, October 16, 2013 7:42 AM

**To:** [REDACTED]

**Subject:** Re: Computer

b6  
b7C

Not sure what you did but it works after 35 times of trying!

[Quoted text hidden]

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1353814-0

Total Deleted Page(s) = 60

Page 6 ~ Duplicate;

Page 7 ~ Duplicate;

Page 9 ~ b1 - Per Dos; b6 - Per Dos; b7C - Per Dos; b7E - Per Dos;

Page 10 ~ b1 - Per Dos; b6 - Per Dos; b7C - Per Dos; b7E - Per Dos;

Page 11 ~ b1 - Per Dos; b6 - Per Dos; b7C - Per Dos; b7E - Per Dos;

Page 12 ~ b1 - Per Dos; b6 - Per Dos; b7E - Per Dos;

Page 13 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 14 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 15 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 16 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 17 ~ b1 - Per DOS; b6 - Per DOS; b7E - Per DOS;

Page 18 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 19 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 20 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 21 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 22 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 23 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 24 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 25 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 26 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 27 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 28 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 29 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 31 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 32 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 33 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 34 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 35 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 36 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 37 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 38 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 39 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 40 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 41 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 42 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 43 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 44 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 45 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 46 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 47 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 48 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 49 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 50 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 51 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 52 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 53 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 54 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 55 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

Page 56 ~ b1 - Per DOS; b7E - Per DOS;  
Page 57 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 58 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 59 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 60 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 61 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 62 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 63 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 64 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 65 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 66 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;  
Page 67 ~ b1 - Per DOS; b6 - Per DOS; b7C - Per DOS; b7E - Per DOS;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

- PRES PRO

Field Office Acquiring Evidence WFO

Serial # of Originating Document

29

Date Received

10-29-15

From

[Redacted]

(Name of Contributor/Interviewee)

DS/IL/CI

(Address)

Arlington VA

(City and State)

By

[Redacted]

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1 A 21

Title: Midyear Exam

Reference:

DS

[Redacted]

(IL) & Signed SF-312(5)

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

DS

[Redacted]

(IL) & Signed SF-312(5)

HRC-6303



United States Department of State

Washington, D.C. 20520

October 29, 2015

**MEMORANDUM**

**TO:** FBI - [redacted]

b6  
b7C

**FROM:** DS/ICI/CI - [redacted]

b6 Per  
b7C DOS

**SUBJECT:** Receipt of Files Transfer for DS/ICI/CI Case **PI-00-US-15-57**

This memo serves as a transfer receipt from the Diplomatic Security Counterintelligence Division to the Federal Bureau of Investigations for the following items:

- Personal files of [redacted]
- Personal files of [redacted]
- Personal files of [redacted]
- Personal files of [redacted]
- Personal Files of [redacted]
- Personal files of [redacted]

b6  
b7C

- [redacted] database search results responsive to the October 6 record request; and
- Signed SF-312 forms responsive to the October 6 record request.

b7E Per DOS

Signature below acknowledges receipt on behalf of the FBI:

[redacted signature box]

b6  
b7C

10-29-15  
Date

UNCLASSIFIED

HRC-6304



United States Department of State

Washington, D.C. 20520

October 15, 2015

~~(SECRET//NOFORN)~~  
MEMORANDUM

TO: DS/ICI/CI - [ ] Investigations Division Chief  
THROUGH: DS/ICI/CI - [ ] NASA Section Chief  
FROM: DS/ICI/CI - [ ]  
SUBJECT: PI-00-US-15-57  
FBI 811 request for Production of Records:

b6 Per  
b7C DOS

~~(S//NF)~~ On 06 October 2015, DS/ICI/CI received a request for DS/ICI/CI database records for 35 State Department records in. The information was requested to satisfy a Section 811(c) that the FBI received from the Inspector General of the Intelligence Community.

b1 Per Dos  
b6 Per Dos  
b7E Per Dos

~~(S//NF)~~ In furtherance of this investigation DS/ICI/CI was able to find records in [ ] (S)  
[ ] for 16 of the 35 subjects. The employees  
with records found were [ ]

b6  
b7C

~~(S//NF)~~ A special note: [ ]  
[ ]

b6 Per  
b7C DOS

~~(S//NF)~~ DS/ICI/CI was only able to find five signed SF-312 forms from the October 6, 2015 addition; [ ]  
[ ]

b6  
b7C

~~(S//NF)~~ DS/ICI/CI has attached all of the found records from the employees.

APPROVED: [ ] 10/15/15 DISAPPROVED: [ ]  
(Initial and Date) (Initial and Date)

b6 Per  
b7C DOS

~~(SECRET//NOFORN)~~  
Classified by [ ] Division Chief DS/ICI/CI  
Reason: 1.4c; Declassify: 10/15/2040

HRC-6305

FBI-811

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-09-2016 BY J76J18T80 NSIDG

HRC-6306



HRC-6309

~~SECRET/NOFORN~~

BUREAU OF DIPLOMATIC SECURITY

b1 Per DOS  
b6 Per DOS  
b7C Per DOS

(S) **TITLE** Counterintelligence Debriefings of U.S.  
Employees, American Embassy

**CASE CLASSIFICATION**

**FIELD OFFICE**  
DS/CMI/CI(EFY)

**DATE REPORTED**  
08/25/93

**DATES INVESTIGATED**  
Since 1/1/92

**REPORTING AGENT**

**SYNOPSIS**

(S) [redacted] During CY 1992, approximately 48 employees departed post after completing a permanent change of station or a temporary duty assignment. The employees interviewed represented various U.S. government civilian and military agencies, and they were either interviewed by Special Agents of the Diplomatic Security Service or by Security officials of the other U.S. government agencies. Reports of interviews are normally required, and copies are to be sent to the Regional Security Officer at the employees' last post. In addition to conducting the interviews, DS/CMI/CI officers tracked the employees to their new assignments (when possible) to insure that debriefings were completed. If information requiring additional investigation or follow-up was developed this office made every effort to see that it was done. Developed leads were forwarded to RSOs, other Federal agencies and other interested parties. All reports, related letters, memoranda, and correspondences are filed in the case file. Attached to this form is a list of the employees who were tracked and interviewed. This case is considered closed.

b1 Per DOS

- CLOSED -

(S) **REFERENCE:** [redacted]

b1 Per DGS

**APPROVED**

DO NOT WRITE IN THIS SPACE

S/CI

(Special Agent In Charge)

Original DS/CMI/CI

(S) **COPIES REFERRED**

1

Date Received

b1 Per DOS

**REVIEWED BY AGENT SUPERVISOR**

(Date)

(Initials)

50249-101

~~SECRET/NOFORN~~

(Formerly DS-838)  
OPTIONAL FORM 249  
MARCH 1975  
DEPT. OF STATE

~~CONTENT MUST NOT BE DISCLOSED TO UNAUTHORIZED PERSONS~~

HRC-6331



United States Department of State

Washington, D.C. 20520

March 15, 1993

~~CONFIDENTIAL~~  
MEMORANDUM

TO: DS/CMI/CI - Mr. [REDACTED]  
FROM: ICS - John J. Stein [initials]  
SUBJECT: SY-56-RS-92-151 (Missing Classified)  
Request to Close Case File

b6 Per  
b7C DOS

92 Moscow 35238 advised that several confidential documents were missing from the files of political officer [REDACTED]

Subsequent investigation by DS/CR/SI and RSO Moscow indicated that the documents probably never left the core, and the political section damage assessment indicated that the documents may have been inadvertently shredded. DS/CR/SI considers the matter closed. Consultations with DS/CR/SI and a review of the case papers did not surface anything of CI interest.

b6  
b7C

No further CI action warranted. Request case be closed.

APPROVE [initials]

DISAPPROVE \_\_\_\_\_

DATE: [initials]

~~CONFIDENTIAL~~  
DECL:OADR

Drafted: [REDACTED]

b6 Per  
b7C DOS

HRC-6369



United States Department of State

Washington, D.C. 20520

October 15, 2015

~~SECRET//NOFORN~~  
MEMORANDUM

TO: DS/ICI/CI - [ ] Investigations Division Chief  
THROUGH: DS/ICI/CI - [ ] NASA Section Chief  
FROM: DS/ICI/CI - [ ]  
SUBJECT: PI-00-US-15-57  
FBI 811 request for Production of Records:

b6 Per  
b7C DOS

~~(S//NF)~~ On 06 October 2015, DS/ICI/CI received a request for DS/ICI/CI database records for 35 State Department records in. The information was requested to satisfy a Section 811(c) that the FBI received from the Inspector General of the Intelligence Community.

~~(S//NF)~~ In furtherance of this investigation DS/ICI/CI was able to find the employee records for 16 of the 35 subjects. The employees with records found were [ ]

b6  
b7C

~~(S//NF)~~ A special note: [ ]

b6 Per  
b7C DOS

~~(S//NF)~~ DS/ICI/CI was unable to find any signed SF-312 forms for everyone on the October 6, 2015 addition except for [ ]

b6  
b7C

~~(S//NF)~~ DS/ICI/CI has attached all of the found records from the employees.

APPROVED: \_\_\_\_\_ DISAPPROVED: \_\_\_\_\_  
(Initial and Date) (Initial and Date)

~~SECRET//NOFORN~~

Classified by [ ] Division Chief DS/ICI/CI  
Reason: 1.4c; Declassify: 10/15/2040

b6 Per  
b7C DOS

HRC-6370

SF-312

HRC-6371

# CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

b6  
b7c

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, \*952 and 1924, Title 18, United States Code, \*the provisions of Section 783(b), Title 50, United States code, and the provisions of the intelligence Identities Protection Act of 1982. I recognize that nothing in the Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States code (governing disclosures to Congress); Section 1034 of Title 10, United States code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United State Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE \_\_\_\_\_ DATE (mm-dd-yyyy) 02/03-2009 SOCIAL SECURITY NUMBER \_\_\_\_\_ b6 Per DOS  
(See Notice below)  
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)  
(Type or print)

Circle one: GS FS PSC WAE Contractor Intern Other \_\_\_\_\_

Bureau Assigned: S Telephone: ( ) -

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIG _____	DATE (mm-dd-yyyy) <u>02-03-2009</u>	SIG _____	DATE (mm-dd-yyyy) <u>02-03-2009</u>
NAME AND ADDRESS (Type or print) <u>SA-20, 13th fl. DS/IS/APD</u> <u>1801 North Lynn Street,</u> <u>Arlington, Virginia 22209</u> <u>571-345-3066</u>		NAME AND ADDRESS (Type or print) <u>SA-20, 13th fl. DS/IS/APD</u> <u>1801 North Lynn Street,</u> <u>Arlington, Virginia 22209</u> <u>571-345-3066</u>	

### SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE \_\_\_\_\_ DATE (mm-dd-yyyy) \_\_\_\_\_  
NAME OF WITNESS (Type or print) \_\_\_\_\_ SIGNATURE OF WITNESS \_\_\_\_\_

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that approval for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) verify that you have access to the information indicated above or 2) determine that your access to the information indicated has been terminated. Although the disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

HRC-6373

# CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND UNITED STATES

(Printed or typed)

b6  
b7c

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, \*952 and 1924, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States code, and the provisions of the intelligence Identities Protection Act of 1982. I recognize that nothing in the Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)



10. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 2.2 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 894, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the information referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so

b6 Per DOS

SIGNATURE	DATE (mm-dd-yyyy)	SOCIAL SECURITY NUMBER (See Notice below)
	02-27-2009	
ORGANIZATION (Type or print)	PROVIDE: NAME, ADDRESS, AND IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER	

Circle one: GS FS PSC WAE Contractor Intern Other

Bureau Assigned: Telephone: ( ) -

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.
DATE (mm-dd-yyyy)	DATE (mm-dd-yyyy)
02-27-2009	02-27-2009
NAME AND ADDRESS (Type or print)	NAME AND ADDRESS (Type or print)
SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066	SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066

b6 Per  
b7C DOS

SECURITY DEBRIEFING ACKNOWLEDGMENT	
I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been returned to the organization; that I will not communicate or transmit classified information to any unauthorized person; and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.	
SIGNATURE OF	DATE (mm-dd-yyyy)
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

b6 Per  
b7C DOS

NOTICE: The Privacy Act, 5 U.S.C. 552e, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

\*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

HRC-6375

# CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

b6  
b7c

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, \*952 and 1924, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in the Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.


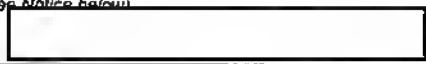
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)





10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE (mm-dd-yyyy)	SOCIAL SECURITY NUMBER (See Notice below)	b6 Per DOS
	NOV 17 2008		
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)			


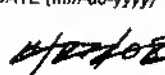

Circle one: GS PS PSC WAE Contractor Intern Other ☒

Bureau Assigned: 5110000000 Telephone: (202) 647-5633

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
	DATE (mm-dd-yyyy) NOV 17 2008		DATE (mm-dd-yyyy) NOV 17 2008
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	
 SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066		 SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066	

#### SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE (mm-dd-yyyy)	b6 b7C
		
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS	
		

**NOTICE:** The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

\*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

# CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of individual - printed or typed)

b6  
b7c

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession, or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

HRC-6378

(Continue on reverse.)

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE		DATE	9/16/99	SOCIAL SECURITY NUMBER (See Notice below)	b6 Per DOS
ORGANIZATION	I, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)				

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT. b6 Per b7C DOS	
SIGNATURE	DATE	SIGNATURE	DATE
	SEP 17 1999		SEP 17 1999
 [Signature Box]  DS/ISP/APB Department of State 2201 C Street, N.W. Washington, D.C. 20520		 [Signature Box]  DS/ISP/APB Department of State 2201 C Street, N.W. Washington, D.C. 20520	

### SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certification or determinations, or possibly result in the denial of your being granted access to classified information.

\* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-91)

HRC-6379

## CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

b6  
b7c

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, \*952 and 1924, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in the Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, or may result, from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)



10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States code (governing disclosures to Congress); Section 1034 of Title 10, United States code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (3) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

<div style="border: 1px solid black; width: 150px; height: 40px;"></div> (Type or print)	DATE (mm-dd-yyyy)	SOCIAL SECURITY NUMBER (See Notice below)	b6 Per DOS
	01-26-2009	<div style="border: 1px solid black; width: 150px; height: 20px;"></div>	
EMPLOYEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)			

Circle one: GS FS PSC WAE Contractor Intern Other\_\_

Person Assigned: S Telephone: ( ) -

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
<div style="border: 1px solid black; width: 250px; height: 40px;"></div> NAME AND ADDRESS (Type or print)	DATE (mm-dd-yyyy) 01-26-2009	<div style="border: 1px solid black; width: 250px; height: 40px;"></div> NAME AND ADDRESS (Type or print)	DATE (mm-dd-yyyy) 01-26-2009
SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066		SA-20, 13th fl. DS/IS/APD 1801 North Lynn Street, Arlington, Virginia 22209 571-345-3066	

#### SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I ~~have~~ (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE (mm-dd-yyyy)
<div style="border: 1px solid black; width: 100%; height: 40px;"></div>	
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS
<div style="border: 1px solid black; width: 100%; height: 40px;"></div>	

**NOTICE:** The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

\*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

HRC-6381

HRC-6382